Yuqing Zhai

10/02/2024

In 2018, the FBI started an operation 'Trojan Shield'. FBI made a secure messaging app ANOM used by criminals to send copies of all the messages to law enforcement. To obviate 4th Amendment objection, the message was first sent to Australia, and then to the FBI using Mutual Legal Assistance Treaty (MLAT). [1, 3] **This essay will argue that this operation is unethical using deontological ethics.**

Deontological ethics judges actions based on one's intent to fulfill the duty to others, emphasizing 'good will' as defined by Immanuel Kant. In the case of government law enforcement, although it has the responsibility to catch criminals, it also has the duty to respect the privacy and autonomy of citizens granted by the Constitution during operations. FBI collects the information by deliberately tricking users into thinking that they are communicating securely. [1] Furthermore, to circumvent the 4th amendment, the FBI sent the data first into Australia and then back to itself. **This behavior shows that the FBI does not have the 'good will' to fulfill its duty to citizens' privacy, and therefore unethical by deontological ethics.**

One legal concept that might justify the operation Trojan Shield is the third-party doctrine, which holds that individuals lose their reasonable expectation of privacy when they voluntarily give information to a third-party entity, and therefore, law enforcement could retrieve the data from the third party without the warrant given from the court. This doctrine could be used in defending the retrieval of the information by the FBI from the ANOM's data in Australia. However, as ANOM advertises as the 'secure messaging app', users are not asked to share their communications via a Term of Service, and they never know their communications are shared with law enforcement. There is no loss of reasonable expectation of privacy of the communication data when users use the ANOM. **Thus, the third-party doctrine does not apply here, and the FBI's action cannot be justified by third-party doctrine.**

The use of ANOM should be considered as a 4th Amendment search. The use of ANOM could be regarded as somewhat like intentional interception of electronic communications. **If a civilian collects data in this way, it's likely to violate privacy laws like the Electronic Communications Privacy Act (ECPA)**. It prevents the intentional interception of electronic communication in transit, which is what the FBI did in this case. Laws like the ECPA and the Stored Communication Act (SCA) all require legal agencies to get a subpoena or warrant from a court in most cases to acquire information from a third party. [2] The subpoena requires reasonable relevance, and the warrant requires probable cause to the cases that law enforcement is investigating. The idea is

that law enforcement cannot search unless they have reasonable suspicion that getting one piece of private information is beneficial to the investigation. In this sense, as an operation like ANOM collects private communications from individuals, **it must require a warrant to do so.**

Reference

[1]

Cox, J. (2021, July 7). Trojan Shield: How the FBI Secretly Ran a Phone Network for Criminals. https://www.vice.com/en/article/operation-trojan-shield-anom-fbi-secret-phone-network/

[2]

Bureau of Justice Assistance. (n.d.). Electronic Communications Privacy Act of 1986 (ECPA). https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#3-0

[3]

Cox, J. (2023, July 24). Defense Lawyers Push Judge to Reveal Secret Country that Helped FBI Wiretap the World. https://www.vice.com/en/article/defense-lawyers-push-judge-to-reveal-secret-country-that-helped-fbi-wiretap-the-world/