How the US SAFE WEB Act Would Help the FTC: A Hypothetical Spyware Case[1]

The FTC receives several consumer complaints about a particular spyware program and sees several news reports about how this program is being used to steal consumer data. The program is also causing many consumers' computers to crash. The FTC begins investigating by finding the website that launched the spyware program. It learns the Internet Protocol (IP) number for the computer that registered the website, and learns the identity of the Internet (essentially, an investigative subpoena) to the ISP to find out who the ISP's customer is.

The ISP turns over the relevant information about the sub-leasee of the IP block. Based on the information provided, the FTC does not learn the identity of the ultimate spyware operator. Rather, the FTC learns that the IP block was sub-leased to a Romanian ISP. Unbeknownst to the FTC, the U.S.-based ISP has informed the Romanian ISP that the FTC is investigating, and the Romanian ISP has in turn informed the spyware operator. At this point, the spyware operator has learned about the FTC's investigation, so he shuts down his websites and creates new ones, thereby thwarting the FTC's investigation. At the same time he takes steps to transfer his money from a bank with a U.S. branch to a Caribbean bank he feels sure is out of the FTC's reach.

The US SAFE WEB Act could have prevented this result: It would allow a judge to require the U.S.-based ISP to keep the FTC's investigation confidential for a limited period of time.

Assuming that the spyware operator was not notified, now the FTC has information about the Romanian ISP that sub-leased some IP numbers from the domestic ISP. But the FTC has no effective way of compelling the Romanian ISP to turn over the information about its customer. So FTC staff decides to seek assistance from the Romanian consumer protection agency. The Romanian consumer protection agency agrees to open its own investigation, but only on the condition that it can have access to the FTC's files about this investigation, including the written responses to the CID that the FTC sent to the U.S.-based ISP. The FTC cannot turn over the written CID responses. Thus, the Romanian agency does not act, and the FTC must abandon its investigation because it has no other leads.

The US SAFE WEB Act could have prevented this result: It would allow the FTC to share the information it obtained through the CID with the Romanian agency.

---

1. This paper illustrates ways in which the US SAFE WEB Act could help the FTC in a hypothetical spyware investigation. Although the specific fact-pattern is fictional, it is based on problems the FTC has encountered in several separate investigations.

The US SAFE WEB Act could have facilitated enforcement by allowing FTC attorneys to be detailed to DOJ to work on this type of case, thus providing additional resources to DOJ to seek enforcement.

FTC's litigation against Hotweb is complete, but the U.K. Office of Fair Trading (OFT) is investigating a similar spyware operation in the U.K. called Coldweb, that is affecting both U.S. and U.K. consumers. The OFT learns that Coldweb has employed U.S.-based ISPs to host its websites, and the OFT would like the FTC to compel the ISP to disclose information about its customer. It asks the FTC for help. The FTC must decline. The OFT offers to reimburse the FTC for expenses associated with finding the necessary information. The FTC cannot accept this offer.

The US SAFE WEB Act could have prevented this by allowing the FTC to send a CID or subpoena to the U.S.-based ISPs in support of the OFT action. It would also allow the