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 Service Provider (ISP) that owns the particular block of IP numbers at issue. In this case, the ISP is based in the United States, so the FTC sends a Civil Investigative Demand, or CID (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.

Assume that the FTC got the information it needed and found the spyware operator, a company named Hotweb, based in Canada. At this point, FTC investigators need more information about how the spyware program operates. They find that Competition Bureau Canada had conducted a similar investigation into Hotweb. The FTC asks its Competition Bureau colleagues for relevant information. Competition Bureau Canada will only share the information if the FTC can assure the confidentiality of the information, even after its investigation is over. The FTC cannot, so the Competition Bureau cannot share this information.

The US SAFE WEB Act could have prevented this result: It would allow the FTC to give the Competition Bureau assurances of confidentiality so that the FTC could have obtained the relevant information.

At this point, assume the FTC has the information it needs to file a lawsuit. It files a complaint and request for a Temporary Restraining Order against Hotweb in U.S. court. Hotweb responds, and argues that the FTC has no jurisdiction over a foreign entity such as Hotweb. Although the FTC ultimately prevails, it expends significant resources litigating this issue.

The US SAFE WEB Act could have prevented this by expressly confirming the scope of FTC jurisdiction.

The FTC obtains a Temporary Restraining Order against Hotweb in a U.S. court. Now, the FTC is looking for information about Hotweb's assets so that they can be used for consumer redress. A Canadian financial regulator has some information about Hotweb's assets in Canada, but will only share that information with a foreign agency if there is a reasonable likelihood that sharing the information will lead to criminal prosecution. The Canadian regulator looks at the FTC statute and sees no reference to criminal matters for this type of investigation, and thus does not share the information.

The US SAFE WEB Act could have prevented this result: It would specifically authorize the FTC to make criminal referrals, which would signal to foreign agencies that their cooperation with us could lead to criminal prosecution.

The FTC also asks the U.S. federal banking agencies for information about Hotweb's potential assets in the United States, which would make recovering money for consumers much easier. The federal banking agencies have a Suspicious Activity Report involving a bank account affiliated with Hotweb, but cannot share this report with the FTC.

The US SAFE WEB Act could have prevented this result: It would authorize the federal banking agencies to share this report with the FTC.

The FTC obtains a final judgment against Hotweb in the amount of $1 million, but Hotweb only has assets in Canada. The FTC requests that the Department of Justice ("DOJ") try to enforce the judgment in Canada, which is a costly and time-consuming process.

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 FTC to accept reimbursement for its assistance to the OFT.

The Hotweb and Coldweb investigations are over, but during an international meeting of the International Consumer Protection and Enforcement Network (ICPEN), a network of consumer protection enforcement agencies from over 30 countries, agency representatives share their experiences and learn that Hotweb, Coldweb, and other companies have simply bought software from a spyware kingpin. No one knows the location of this kingpin. ICPEN members decide to pool their resources to hire someone to (1) work with individual countries on investigations and (2) set up an Intranet site to share leads. The FTC cannot currently contribute to the pool of resources.

The US SAFE WEB Act could have prevented this by allowing the FTC to contribute funds for this and other ICPEN projects.

Lack of U.S. funding stalled the ICPEN project, so the OFT proposes sending an OFT investigator to Washington to work directly with an FTC investigator on joint investigations into spyware operators. This way, the expertise of the OFT and FTC could be pooled in further investigations. Currently, the FTC cannot accept this offer.

The US SAFE WEB Act could have prevented this by allowing for staff exchanges between the FTC and officials from relevant foreign agencies.

In a meeting between the FTC and a U.S.-based ISP, the ISP reveals that it has received several customer complaints about spyware operators like Hotweb, and it continues to receive such complaints on an ongoing basis. FTC staff asks if the ISP can send these complaints to the FTC on a regular basis, and the ISP says it will not, because it is concerned about being sued.

The US SAFE WEB Act could have prevented this by exempting ISPs from liability for sharing complaints with the FTC.