Comments on FTC's Draft Compalint and Proposed Consent Order Involving Twitter
By, Russ Smith, CISSP

I have reviewed the FTC's draft complaint and consent order involving Twitter and I wish to file public comments. I operate web sites such as Privacy.net and I have held a Certified Information Systems Security Professional (CISSP) certification since 2001. I am not being paid to submit these comments by any I do not represent any other party or entity.

The complaint and consent order involve a number of claimed "best practices.[1]" The practices are similar to those that are supposed to be used by Federal agencies.[2] The FTC has no legal authority to enforce such "best practices" and the FTC staff does not have the expertise to do so. The FTC staff does not have the ability to understand and enforce NIST best practices which is readily apparent from the bare-bones requirements set forth in the Twitter Complaint. For instance, there is a requirement to have complex passwords that change often and have a "lock out" for too many wrong attempts. Depending of the specific situation, this could lead to less security. For instance, if someone is forced to have complex passwords that change often this may cause users to write the password down or use the same password they use for other purposes. However, if there is a sufficient lockout mechanism in place having overly complex passwords that change serves no purpose. This is why NIST has a series of lengthy documents rather than few pages (which, in this case, the purpose appears to be generating a news release rather then implement comprehensive information security).

The FTC staff also does not consider all legal and other ramifications, such as coordinating with other agencies, when conducting these "enforcement by consent order" actions. Information security is balanced with other things, such as privacy and legal requirements, which are not considered by the consent order. Some examples are discussed below.

The FTC also fails to clearly state their authority to enforce what they understand to be "best practices" without considering other ramifications which appears to be a common practice at the FTC. One example is the FTC Spam reports and recommendations[3] where the FTC

---

1 The agency in charge of developing "best practices" is the National Institute of Standards and Technology (NIST) and are found on the "800 series" publications . Special Publications in the 800 series present documents of general interest to the computer security community and was established in 1990 to provide a separate identity for information technology security publications. This series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

2 The E-Government Act (Public Law 107-347). Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

3 Such as Spam Summit: The Next Generation of Threats and Solutions FTC report issues

recommends ISP essentially eavesdrop on customers Internet connections in order to detect spam "zombies" and other security issues. Yet the report fails to even mention or consider the Electronic Communications Privacy Act. Further, at the same time, the FCC was insisting Comcast implement a "protocol agnostic" network management technique in response to the Peer to Peer (P2P) congestion issues[4]. The FTC Spam report also fails to mention how privacy policies and other policies should be adapted to inform users about these procedures. This lack of coordination and haphazard enforcement by the FTC and FCC has lead to me filing litigation against Comcast (and others).[5] This lawsuit has brought out the fact that many major companies, such as Microsoft and Cisco, claim they are not bound by a contractual relationship by their posted privacy policy when a user visits their respective web sites.[6]

November 2007.

4 In this case the FCC, much like FTC consent order being discussed here, was found to have no legal authority to implement such a rule. The judge even stated that when the FCC appeared to defend their actions they failed to identify even one statute where their authority is claimed to have originated. Rather than seek action by Congress as set forth by law, the FCC continues to look for legal loopholes to conduct enforcement in areas of questionable legal authority. Agencies have generally made stuff up as they go along as they attempt to expand their authority and build empires while increasing the deficit.

5 Russ Smith v. TRUSTe, Microsoft, Cisco, and Comcast is in federal court (1:09-cv-04567) and alleges that Comcast breached contracts by issuing a network management policy that states they operate a "protocol agnostic" network management system (in response to FCC action) while, in actuality, Comcast blocks specific ports and applications while they point to FTC best practices. (The complaint alleges that Comcast has used these so-called FTC "best practices" to increase revenue in violation of the NJ Consumer Fraud Act). The cases also alleges Cisco violates the NJ Consumer Fraud Act because they claim to operate a "Credit reporting Service for E-Mail" and issues "Reputation Scores" to IP addresses while not allowing those affected to review or dispute incorrect "bad" reputations.

6 In pleading filed in federal court [Russ Smith v. TRUSTe, Microsoft, Cisco, and Comcast is in federal court (1:09-cv-04567)] Microsoft, Cisco and TRUSTe stated:

"Plaintiffs proposed Amended Complaint alleges that the privacy policies found on the Web sites of Microsoft, Cisco, and TRUSTe constitute contracts between those Defendants and him. … The most cursory review of the documents attached to the proposed Amended Complaint as Exhibits Q-R, V-X, and GG, respectively [privacy policies of Microsoft, Cisco and TRUSTe], demonstrates that they do not constitute enforceable contracts between Plaintiff and Microsoft, or Cisco, or TRUSTe. The documents do not establish privity between Plaintiff and Defendants, an exchange of mutual obligations or consideration, or any manifestation of intent by Defendants to be bound vis-à-vis Plaintiff." (DEFENDANTS' JOINT MEMORADUM OF LAW IN OPPOSITION TO PLAINTIFF'S MOTION FOR LEAVE TO AMEND THE COMPLAINT)

"Plaintiff's assertion that TRUSTe admits that simply visiting its Web site constitutes an exchange of consideration and creates an enforceable contract is baseless. Plaintiff's bare, conclusory allegation that Cisco's, Microsoft's, and TRUSTe's Web sites and privacy

However the FTC has done essentially nothing to educate the public to this. The FTC has also implicitly endorsed the TRUSTe seal program that implies to the public that their seal holders (such as Comcast, Microsoft, and Cisco) are bound by their posted privacy policies when a user visits the web sites of these companies[7].

The FTC and other agencies do not maintain privacy practices that would comply with the consent order issued by the FTC. In fact most agencies fail to provide any coherent response to inquiries about their privacy policies (which can be readily tested by anyone). For instance, I inquired about the FTC privacy policy relating to the National Do Not Call registry.[8] The FTC is aware the information in the registry has been used for other purposes other than do-not-call. Not only won't the FTC disclose what has been detected, they state in their policy this does not happen. Further, other information is collected from third parties, such as telephone records, and combined with the data collected by do-not-call submissions. The FTC does not disclose this as required in the Privacy Act disclosures and would not provide the information even after I submitted a FOIA request.[9]

I have also filed numerous inquiries and complaints about federal web sites that use services such as Twitter, Facebook, and Youtube and other third parties (such as a comment collection system used by the FCC). The problems are that (a) agencies fail to coordinate and disclose in their privacy policies what happens to information collected, (b) agencies fail to explain how they are using these services without contracts, and (c) whether use of these services effectively advertising/promoting private services in violation of the policy for use of ".gov" domain names.[10] These inquiries include complaints filed with the OIG offices of both the FTC and FCC which were never answered coherently.

Large numbers of government sites are using things like Facebook and embedding YouTube

---

policies constitute contracts with him is plainly insufficient to state a claim, and therefore, the breach of contract claims should be dismissed." (DEFENDANTS' JOINT REPLY MEMORANDUM OF LAW IN FURTHER SUPPORT OF THEIR MOTIONS TO DISMISS).

7 TRUSTe routinely associates with regulatory staff such as the FTC. TRUSTe has hired several high level staff members from agencies such as the FTC, DOC and Homeland Security apparently based on these associations. In one case an FTC staff member who was instrumental in endorsing the formation of TRUSTe, Martha Landesberg, was hired directly after leaving the FTC and became TRUSTe's director of compliance for many years. This gives the appearance of protection racket were complaints against those that pay TRUSTe are given a free ride while others, like Twitter, that do not pay for the seal are subject to FTC formal action that has no legal basis.

8 The FTC chose me to testify at a Do Not Call Workshop for the development of the Registry.

9 When I complained about this and submitted a complaint to the FTC's Office of Inspector General (OIG) Office I detected FTC staff searching for information about who I was. I submitted another FOIA request to find out what information they had compiled about me and the FTC never responded to that FOIA request at all (submitted February 6, 2010).

10 The policy is at http://www.dotgov.gov/program_guidelines.aspx

videos in their web sites. I have never seen a government privacy policy that fully explains what information is transferred to third parties and how it is coordinated with these private company privacy policies. I have never received a response to my inquiry that using something like Facebook is effectively an endorsement for this service over other competing services (such as MySpace) and whether there was a competitive process to contract with these companies to use these services. The FCC is now using a commercial web site to collect some comments about their enforcement actions and other matters yet they will not answer privacy policy inquiries about how the information handled. Inquiries to the contractor lead to incomplete and incoherent responses (which is is the norm with privacy policy inquiries).

Now the FTC is effectively trying to tell Twitter to follow FISMA guidelines so agencies can continue to use the service free of charge with no contracts in place. As a result, the FTC and other agencies should pay Twitter to implement the FISMA guidelines proposed in the consent order.

Submitted,

Russ Smith
June 25, 2010