Comment in Response to a Proposed Framework for Consumer Privacy:

Federal Trade Commission
Title: Federal Trade Commission (Bureau of Consumer Protection) Staff Report
Subject Category: A Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

Submitted by

Michael Honchar

February 18, 2011

The proposed framework for privacy proceeds from the acceptance of the current methodologies for tracking consumer and expectation that they will continued to be used. The types of methods which I am aware of that are used by profit-driven organizations such as Microsoft, Yahoo, Google, and others are equally available to a multitude of nations, terrorist groups, and criminal enterprises. It is not conceptually difficult and I think within the range of resources available to likely adversaries to establish a tactical tracking network sufficient to identify and attack computers in government, military, financial, and infrastructural organizations. A tactical, attack oriented network does not need to be as extensive, comprehensive, or expensive as a commercial network since only one or at most a few computers in a targeted system must be identified and attacked in order to deliver a software payload to all computers in the associated network. The problems of protocols for safe handling of commercially collected data seems trivial in comparison to the threat from those likely to use (and I suspect already use) the same methods of tracking users to disrupt government activities and infrastructure functions. I am forced to ask why an advertising-based business model employed by corporations using Microsoft related software is important enough to justify the persistence of the vulnerability which tracking methodologies require or, more concisely, are you people out of your God-damned minds?

Recent revelations by software suppliers about what and where data was being stored on user's machines suggested that old technology was being abandoned for something better for tracking and worse for my nerves. Last year I planned to drop in on some political sites where discussions occasionally became "heated" and felt it was prudent to isolate tracking processes from my physical address. Microsoft was reported to have provided tracking access to user machines but I didn't find any useful details. I started a practice of sanitizing my computer by deleting the subdirectories in the temporary internet file directory and any cache or temporary file that caught my eye before I went to Yahoo/ATT my ISP and after. In effect, I always came with a different computer that had never been seen before and that would never be seen again. After about three weeks Yahoo started sending beacon bomb emails with text similar to, “We haven’t heard from you in a while, click here to check your preferences” and a mass of graphics with tracking links to BellSouth, ATDMT, Yimg and others. I was touched. They ARE watching, they missed me and they came looking. There were about a dozen such emails with increasing enthusiasm levels leading to “Click here and you will enrolled in a $5,000 drawing”. I figured to hold out for dinner, a show and a special desert but the emails just ended I assume because I am in the old guy “Who cares?” demographic. It does look like Microsoft has given websites the ability to peak at some stable identification in user machines and folks like Yahoo are having a ball peeking up users’ skirts.

Once you see this system, it doesn’t take a bit wrangler extraordinaire to see an angle. There are a number of significant “groups” who would be thrilled to knock the US down a few notches for a forced feeding of humble pie and some folks with giant coffers who would probably prefer an end-point involving smoking rubble. As a hypothetical, someone with a plan might buy, establish, or compromise small internet service providers for small businesses in the vicinity of government installations, military bases and some interesting infrastructure like the Calloway nuclear tea pot. The guy at the server would soon have name, rank, serial numbers, and computer tracking numbers for an interesting population of sergeants, majors, directors, engineers and mechanics through reservations, flower orders, pizza deliveries, etc. He would have a good life from the profit of his subsidized business as long as he passes machine data up to an aggregator for relay back some old country or another.

South east Europe has been the studio and stable for Team Rodina for many decades. The area is dirt poor so an artist can get some remarkable photos with petty cash. Thailand, once the land of special vacations with the little people, seems to involve mostly old-style independent contractors but I wouldn’t be surprised if they had updated to the computer age with help from the Kingdom of the North Studios to help provide an outlet for their product. I suspect that a server with some really disgusting artwork and a list of computer tracking numbers would be like spamming; big profits from infinitesimally small returns. Then again, last year there were something like 150 individuals working or stationed at the Pentagon who had paid for and downloaded child pornography to government servers. I don’t remember how many were caught peeking at free-bees. Free-bees are the slow loading high resolution images which cover the simultaneous download of the new HTML GIF and JPG “image” files which are disguised javascript payloads which will certainly work well on your network especially if you have privileges of say a Major or GS-14. A friend retired as an officer from the Army Reserve but stayed for some contract time convincing drivers that if they drove in the sandbox with their head back on a sandbar in the Current River instead of soldier tight under their K-pot they wasn’t going to see that sandbar again. At Fort Riley training involved elaborate simulators which were often attacked from the web and occasionally had to be shut down as a defensive measure.   It seems that one of the computer techs was walked out in handcuffs since he used his real name and credit card to purchase kiddie porn at a site that the Feds had set up on. I don't know if they discovered whether he preferred acrobatics with little girls from the east or bareback stunts from the Caucuses.

The targeting information provided through exposed permanent identification codes in browsers and operating systems is too dangerous to be allowed to exist. The present discussions to control the use of data gathered through such means by legitimate commercial interests ignores the dangers provided by the same methods by hostile groups whose intent is specifically to attack US facilities. I can see no way of limiting such tracking to safe applications. The implementation of this tracking methodology deserves absolute prohibition and felony level penalties. The discussion of the methods of controlling this uncontrollable methodology brings me to my initial question, are you people out of your God-damned minds?