Georgia Tech Ernest Scheller Jr. College of Business

Peter P. Swire
Nancy J. & Lawrence P. Huang Professor
Business Law and Ethics Program
800 West Peachtree St. NW
Atlanta, GA 30308-1149
Peter.swire@scheller.gatech.edu
Phone: 404.385-3279
Fax: 404.894-6030
cob.gatech.edu

March 6, 2016

Professor Nick Feamster
Acting Director
Center for Information Technology Policy
Princeton University
Via email

Dear Nick:

I have read your letter to the FCC and the subsequent blog post in Freedom to Tinker (FTT). I provided an initial response here. On the blog post, I am on board in many ways. Our report was over 120 pages. With that said, our Working Paper necessarily did not cover many topics that may be relevant to the FCC's consideration of broadband privacy. It is notably difficult to explain these topics in a simple and clear way that informs a non-expert audience while being precise enough to satisfy an expert audience.

This letter addresses your blog post in some detail. It then, based on our email exchanges this weekend, briefly summarizes some of your and my views. Based on these email exchanges, our areas of agreement about the facts are considerably greater than first appeared.

To begin, I agree with the facts for the three things you call "missing pieces" in our Working Paper:

1. "A single ISP can still track significant user activities from home network traffic and (as the user moves) through WiFi sharing services."
2. "ISPs can observe user activity based on general traffic patterns (e.g., volumes), unencrypted portions of communication, and the large number of in-home devices that do not encrypt traffic."
3. "DNS traffic sometimes goes to the ISP's DNS server after it exits the VPN tunnel. Configuring certain devices to use VPNs may not be straightforward for many users."

In terms of our Working Paper, I will discuss each of these three points.

Home and WiFi networks. First, our Working Paper, at page 25, makes the same point about how a single ISP may track an individual through WiFi sharing services: "The episodic glimpses are more continuous when the user switches from one connection (such as home) with a particular ISP, and goes to another connection (such as a WiFi hotspot) with the same ISP."

Concerning home usage, we cite to statistics about the relative shift over time from individual user activity on a single home device to multiple devices, which are often mobile. I suspect you agree that a much larger proportion of the typical user's Internet activity today is mobile and out of the home than was true in the early days of the Internet, including sometimes (but sometimes not) hopping to a different ISP at a Wi-Fi hotspot. FWIW, we looked for but did not find useful statistics about how often a WiFi hotspot is the same ISP as home subscription.

Pervasive encryption. Second, for the visibility of an ISP into encrypted traffic, you seem to agree with two things we worked hard on in the Working Paper: (a) statistics showing a large rise in the share of HTTPS traffic in the past two years; and (b) our Diagram 1-A at page 26 showing what is visible to an ISP with the shift to HTTPS. In my experience, many non-experts had not previously had a grasp of Diagram 1-A; that diagram speaks directly to often-voiced concerns about comprehensive Deep Packet Inspection, showing why content is blocked by properly-deployed HTTPS. On the prevalence of encryption, I personally find the most interesting fact in the report the rise of HTTPS traffic from 13% two years ago to 49% today (those statistics come from one data source, but I have found no reason to believe other sources tell a different story).

You state that ISPs can observe general traffic patterns, such as volume, as well as unencrypted traffic, including for a growing number of home devices. I agree entirely, and nothing in our report stated otherwise:

- We repeatedly explain that unencrypted information allows full visibility for an ISP, including in Diagram 1-A.
- Part of my research included a tutorial on Wireshark from someone at Georgia Tech who is proficient in networking, which provided clear visualizations about how number of bits, session length, and other general data is visible to the ISP. My experience and research is that these sources of data are less useful for tracking and online advertising than content or detailed URLs. I would be interested if you or others offer information about how these general sources of data in fact are useful for tracking and online advertising.
- We mention the Internet of Things briefly in the report. I taught Internet of Things cybersecurity in class this week, and share your concern about the lack of encryption and severe lack of overall security for many Internet of Things devices and services. I hope a wide range of technology, policy, and business experts find ways to improve cybersecurity in that realm, and we can note that in the Working Paper. For now, Internet of Things is one portion of home use, which is one portion of an individual's overall Internet-connected activity.

The rising prevalence of encryption (which I have often supported in my writing) is the single strongest basis for one claim of the Working Paper – ISP access to a user's Internet activity (notably including content and deep links) is not "comprehensive" today. Today, content and deep links are blocked for roughly half of traffic, and we expect that fraction to rise. Simply put, ISPs can have "a lot" of visibility into user activity, but not "comprehensive" visibility.

Based on our email exchanges this weekend, you have authorized me to say in this letter that you agree with that last sentence. The genesis of my paper was the FCC public workshop last

April, when some speakers claimed "comprehensive" ISP access and others denied it. I have hoped that a public service of my paper has been to disprove the "comprehensive" description. Whatever the FCC may decide to do, I think it should base its approach on actual visibility rather than "comprehensive" visibility. For instance, if the FCC had mistakenly based a rulemaking on "comprehensive" ISP liability, the factual predicate for its action would have been subject to severe and accurate criticism.

VPNs. Third, concerning VPNs, we carefully created three diagrams and a good deal of text to explain how VPNs work, for a non-expert audience. It seems that you agree in most or all details with this description. One point you make is that VPNs can be configured so that the ISPs' DNS server does in fact see DNS look-up information even though a VPN is in use. That configuration is different than what I learned in briefings about how VPNs operate. I would be glad to get helpful citations from you and clarify that for the Working Paper how configurations differ, including statistics on what is common.

For VPNs you also said: "Configuring certain devices to use VPNs may not be straightforward for many users." Once again, we did not say anything to the contrary. It is true that VPNs have the capability to block even the host name from the ISP, so the destination of a user's web activity can be blocked from the ISP. Our own research suggested that VPN use by individuals has not been especially common in the US, so we did not emphasize this technical limit on ISP visibility nearly as much as the pervasive encryption point. On the other hand, the new services by Facebook and Google may change that in the not-so-distant future. VPNs and proxy servers are a type of limit on ISP visibility.

Conclusion. You published the FTT blog post after the FCC letter. As I think the above discussion shows, the Working Paper is broadly consistent with the three "missing pieces" you highlight; in a number of instances, the Working Paper specifically makes points that you do.

Our email exchanges this weekend, however, also discussed statements in the FCC letter about "many technical inaccuracies" and "basic misunderstandings of various Internet technologies." Based on our email exchanges this weekend, you have authorized me to say in this letter: "Upon more careful review of the paper, I have not found anything in the report that I believe is incorrect. I continue to believe that there are important additional facts that should be considered by policymakers, which were not discussed by the paper."

Thank you for engaging directly on these matters.

/Peter/

Peter Swire