Surprising Facts on ISP Visibility into Internet Activity

Peter Swire
Huang Professor of Law and Ethics
Georgia Institute of Technology
State of the Net 2016
January 25, 2016
Introduction

– A hot topic – role of ISPs in Internet, including what privacy rules should apply

– This research:
  • Description of the facts, not policy recommendations
    – Accurate description is key to good policy
  • Responds to questions raised by FCC when I testified in April hearing on broadband privacy
  • Detailed report expected within a month, with my colleagues Justin Hemmings & Alana Kirkland
  • If anyone sees mistakes in our facts (now or after publication), let us know and we will correct
  • I disagree with two factual statements in privacy groups’ letter last week. I did not see the letter until after it was published, and so could not comment on it pre-publication.
  • I have worked closely with many of the signatories for years. I hope and expect to do so going forward.
Contrasting Views

• Letter last week:

  ISPs have “comprehensive” visibility into user Internet activity

• Our research:

  • No
  • SSL encryption blocks content
  • SSL encryption blocks detailed links
  • Encryption is becoming predominant
Contrasting Views - VPNs

- Letter last week:
  “Nor is there any way for consumers to avoid data collection by the entities that provide Internet access service.”

- Our research:
  - VPNs block ISP access to content and detailed links.
  - VPNs also block top-level URL.
  - Consumers can use VPNs, and many do.
The 1990s and ISPs

1. Desktop at home
2. Unencrypted communications
3. ISP does DNS look-up

All of that has changed, a lot:
1. Multiple devices, often logged in at Wifi spots
2. Encryption
3. VPNs and other proxy services
THE EFFECTS OF HTTPS:

STEP 1 - DNS LOOKUP

I want to visit comfyshoes.com

Can you tell me where comfyshoes is located?

comfyshoes.com
location: 208.67.222.22

Now I know how to locate comfyshoes

comfyshoes is located at 208.67.222.22

ISP

DNS

STEP 2 - CONTENT RETRIEVAL

OVER HTTP

Can you send me to 208.67.222.22?

User can browse comfyshoes

Welcome to ComfyShoes!

ISP retrieves content from 208.67.222.22

ISP delivers content to user

OVER HTTPS

Can you send me to 208.67.222.22?

User can browse comfyshoes

Q29rZnIaG9lcw==

ISP retrieves content from 208.67.222.22

ISP delivers content to user

USER

ISP

COMFY SHOES
WITH VIRTUAL PRIVATE NETWORKS

1. Establishing a connection to a VPN

I want to establish a connection with my VPN

The user wants to establish a secure connection with you.

OK, establish a secure connection with the user

User

Connection with VPN established!

ISP

VPN (proxy server)

ENCRYPTED TUNNEL
WITH VIRTUAL PRIVATE NETWORKS

2. DNS Lookup

USER

I want to go to HTTPS://www.comfyshoes.com

ISP

Forwards encrypted messages between user and VPN

VPN (proxy server)

Decrypts message and performs DNS lookup for IP address of comfyshoes.com

DNS

www.comfyshoes.com is located at 916.47.63.137

In this scenario, the VPN has its own DNS lookup System

LEGEND

WHAT THEY CAN SEE
WWW HOST NAME
FULL URLS CONTENT
WITH VIRTUAL PRIVATE NETWORKS
3. Browsing a Website after the IP address has been retrieved

USER
I want to go to 208.67.222.22
User can browse comfyshoes

ISP
Forwards encrypted messages between user and VPN

VPN (proxy server)
If HTTP
If HTTPS
VPN retrieves content from 208.67.222.22
VPN delivers content to the user

Welcome to: COMFYSHOES.COM!

LEGEND
WHAT THEY CAN SEE
WWW HOST NAME
FULL URLS CONTENT

ENCRYPTED TUNNEL ENCRYPTED TUNNEL
ISPSeeLessThanYouThink

Non-ISPshaveaccess
to substantialuser
onlineinformation

TechnologyblocksISP
Access toTraffic

Individuals use
multiple devices

Individuals use
more than one ISP

ISPs do not have unique visibility
into users’ online activity

+350M New photo uploads by Facebook users each day

2M Websites reaching 90% of Internet users worldwide – Google’s display advertising network

17.3B Desktop search-engine searches in November 2015

$87.5B Estimated quarterly e-commerce sales for third quarter of 2015

+85% People think voice search through digital assistants is the future

$58.6B Projected digital-advertising spending in the U.S. for 2015

Increasing number of onlineadults globally have used a VPN or proxy server to connect to the Internet

More than two-thirds of North American Internet traffic, including the leading online services, will be encrypted in 2016

Number of new worked devices
per person in North America

Internet users with smartphones

Internet users with tablets

Mobile Usage Up
60% Americans time spent online on mobile apps

Wireless Access Points Increasing
454,618 Number of unique U.S. Wi-Fi hotspots tested by Open Signal users in 2014
Conclusion

• These important policy issues should be founded on careful and accurate understanding of today’s (and tomorrow’s) technology and markets
• Encryption applies broadly today to key Internet activities, including:
  – E-commerce
  – Search
  – Social Networks
  – Text messaging (over the top = Internet)
  – Internet video (in 2016)
  – Webmail
• VPNs and other proxy servers are also large and growing
• Claims that ISP have “unique” or “comprehensive” access to user data must be tested against these important facts
Credits

• Images for attribution to Marie Le Pichon, under a Creative Commons Attribution 4.0 license.
• Research support from: Georgia Tech Scheller College of Business; Georgia Tech Institute for Information Security and Privacy; Broadband for America.