It's Too Complicated: The Technological Implications of IP-based Communications on the Content/ Non-Content Distinction and the Third Party Doctrine

Steven M. Bellovin, Matt Blaze,

Susan Landau, Stephanie K. Pell

Wiretap Act Definition of Content

"Contents, when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."

18 U.S.C. § 2510(8)

Wiretap Act Definition of Content

"Contents, when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."

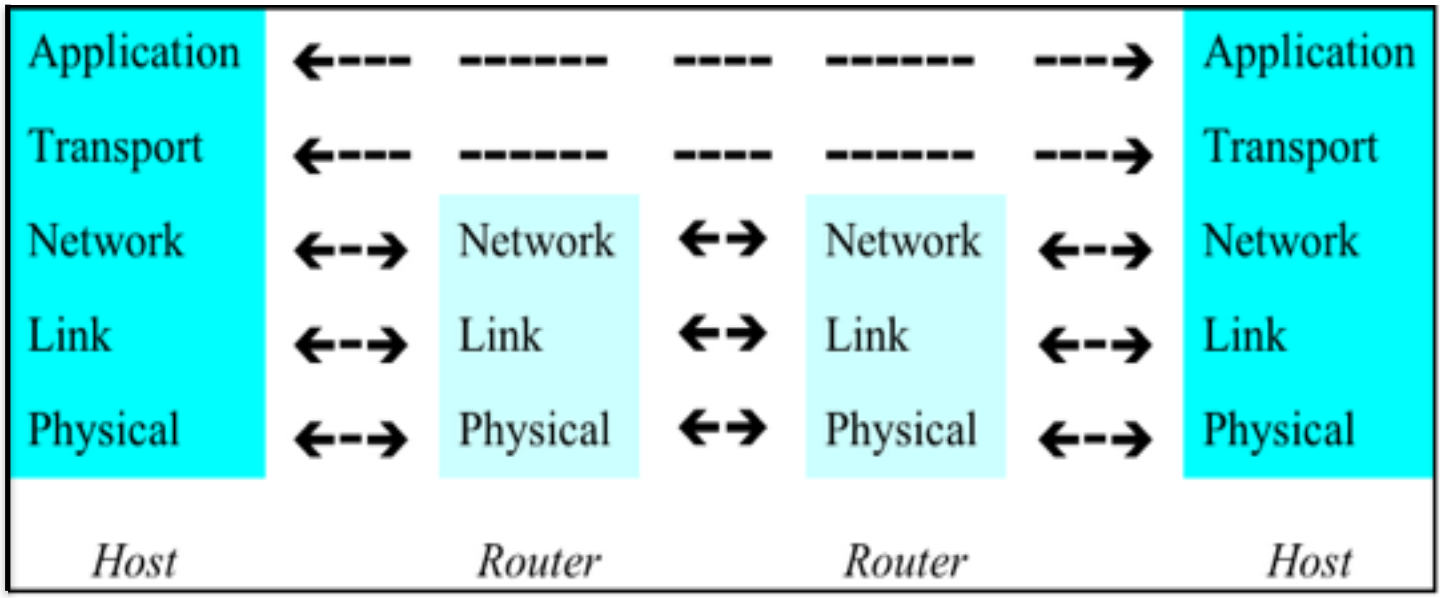
18 U.S.C. § 2510(8)

We call this concept "Communicative Content."

Architectural Content

We use the term *architectural content*, to denote the *unexamined* transportation of a unit of data between two given points in the network. Here, content status is a product of how the network was designed to function as a transport system for application data—that is, how different layers of the Internet are intended to communicate with each other.

The Network Stack



The Internet is organized as *layers*. A layer talks to its peer layer on another computer. The *transport layer* is "end-to-end", *i.e.*, not used by intermediate routers. The *network layer* is used by routers, and thus by ISPs. The transport layer is *architectural content* to the network layer.

From a Court:

“That portion of the "header" which contains the information placed in the header which reveals the e-mail addresses of the persons to whom the e-mail is sent, from whom the e-mail is sent and the e-mail address(es) of any person(s) "cc'd" on the e-mail would certainly be obtainable using a pen register and/or a trap and trace device.”

In re Application of United States,

396 F. Supp. 2d 45, 49 (D. Mass. 2005)

On the Wire

220 yyy.com ESMTP Exim 4.82 Tue, 11 Mar 2014 19:43:03 +0000
HELO xxx.cs.columbia.edu
250 yyy.com Hello xxx.cs.columbia.edu [2001:18d8:ffff:16:12dd:b1ff:feef:8868]
MAIL FROM:<smb@xxx.cs.columbia.edu>
250 OK
RCPT TO:<smb@yyy.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: Barack Obama <president@whitehouse.gov>
To: <smb2132@columbia.edu>
Subject: Test

This is a test
.
250 OK id=1WNSaS-0001z5-1d
QUIT
221 yyy.com closing connection

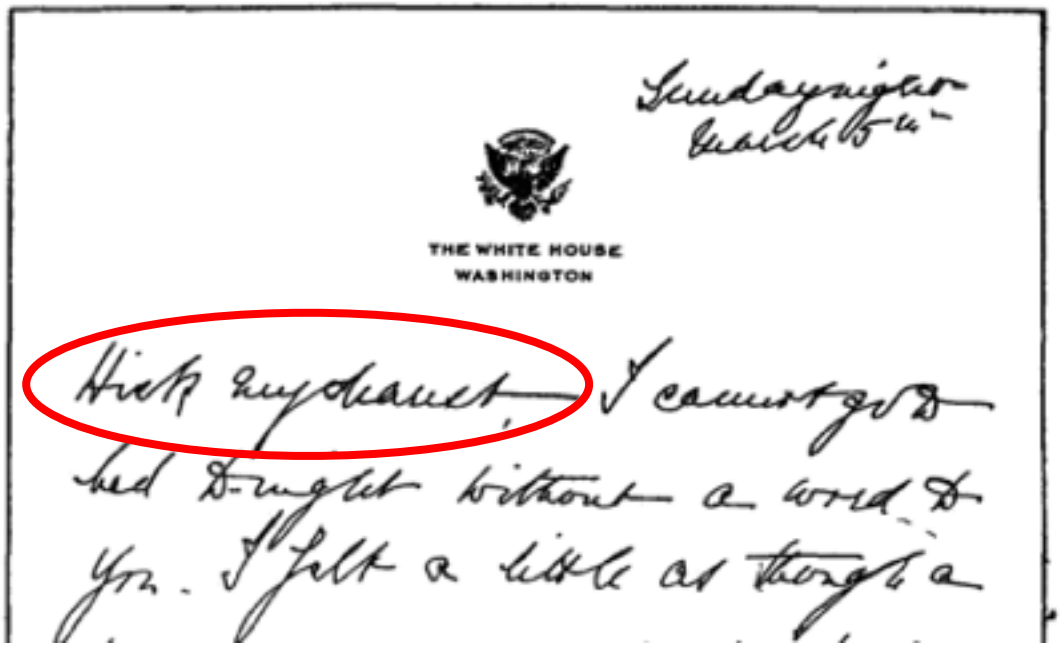
Envelope

Email message contents

SMTP versus the Message

- The SMTP (Simple Mail Transfer Protocol) dialog contains metadata
- The message itself is pure content
- The two sets of recipients need not agree:
  - Bcc –by intent of the sender, the envelope has more information
  - Think of physical envelopes (“Miss Lorena Hickock”) versus the inside salutation (“Hick my Dearest”)

A Letter from Eleanor Roosevelt to Lorena Hicks (March 1933)



THE WHITE HOUSE
WASHINGTON

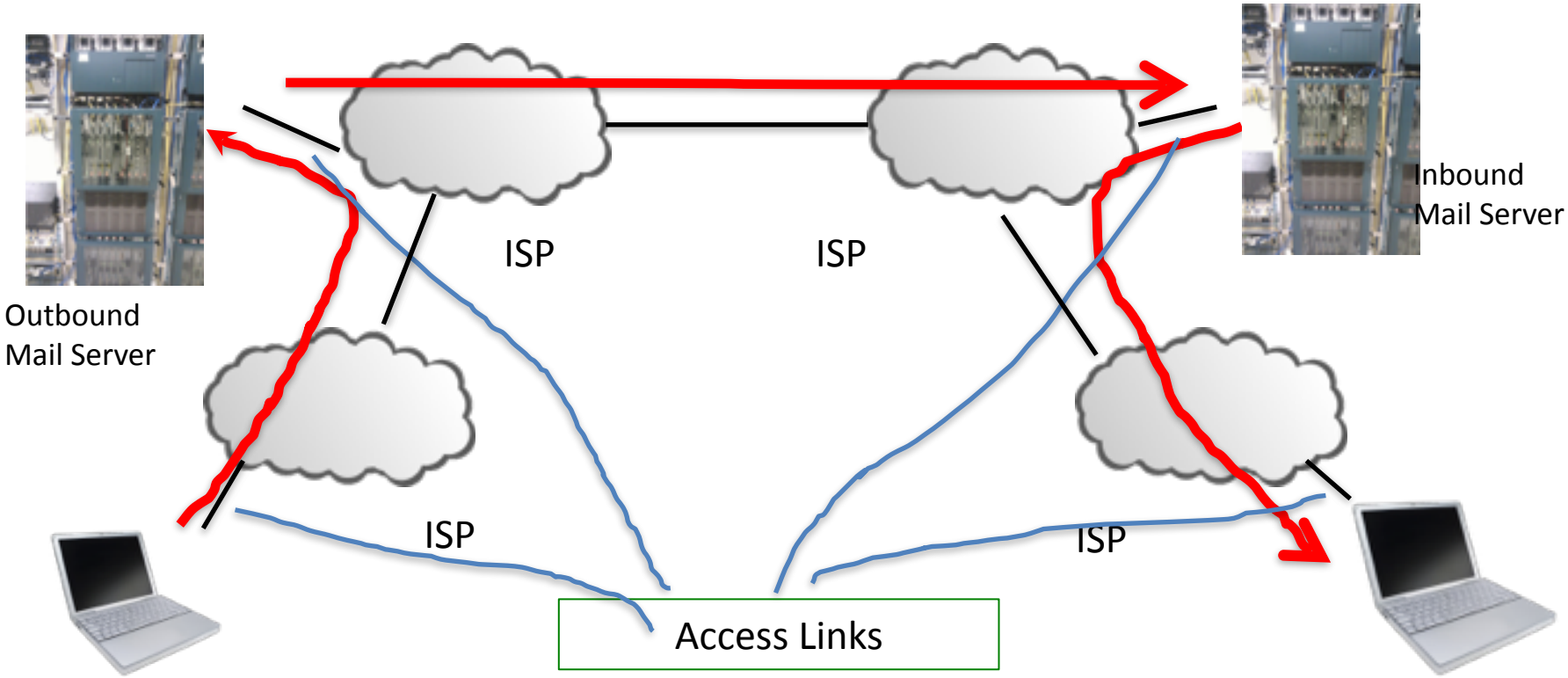
Hick my dearest

(excerpt from Amazon.com)

It begins “Hick my dearest”.

Sending Email

Who owns the mail servers? Is there even a third party involved? (I run my own.)



When is Location Sent?

Location: It's Worse Than That

- Even when online, phones can use cached maps
- Even if not downloading maps, WiFi base station identifiers are sent to the server to aid in location determination
- Standalone GPS units *never* transmit data
- Is the location conveyance "voluntary", per *Smith*?

Voice over IP

- *Ex Parte Jackson* said that the "outward form and weight" of a letter or package was not protected
- White *et al.* showed that they could use packet lengths of *encrypted VoIP* conversations to recover some phrases
- Metadata now reveals content

Conclusions

- We have other (and more complex) examples.
  - Today's Internet is far more complex than it was in its original architecture
- Some information is clearly third party data per *Smith*—but other information is much harder to classify as content or metadata.
- The content/non-content distinction and the third party doctrine are no longer workable rules for an IP-based communications environment. We need new constitutional and statutory frameworks to govern law enforcement access to wire and electronic communications data.