Your on the Street Reporter

Uyless Black

Postal Envelopes and Internet Packets

Postal Envelopes and Internet Packets[1]

Januray 20, 2014

Hello from Your on the Street Reporter. This report continues the series on the subject of privacy and security in the Internet. The essay explains several terms and concepts that pertain to what is called *cyber world* traffic. It will help non-technical readers to better understand the current debates about the privacy of Internet traffic and NSA's so-called snooping of citizens' data.

The table below is explained in more detail in this report. It will serve as a guide in making comparisons between the postal service and the Internet. I recognize some readers might be leery of delving into such details. Don't worry, the material in this report is not technically complex. It is mostly a matter of a new-comer learning a few Internet concepts.

Terms

Postal Service	Internet
Envelope	Packet header
Letter inside envelope	User content inside packet
Street, city, ZIP code	IP address
Mail	Email
Bob	machine.com and Bob.com
188 Anystreet, Anywhere, 88888	192.75.88.5
Placing the letter inside the envelope	Encapsulation

How Traffic is Exchanged between Internet Users

All Internet traffic (voice, video, photos, and text) is exchanged in small packets (envelopes) of digital images. These images are equivalent to conventional words, photos, and video clips, but they are not represented as vocal or visual signals. They take the form of binary numbers (1s or 0s). They are represented with electronic or optical energy levels. The 1s and 0s are strung out in specific combinations of codes to represent say, a spoken or written message, as seen in Figure 1.

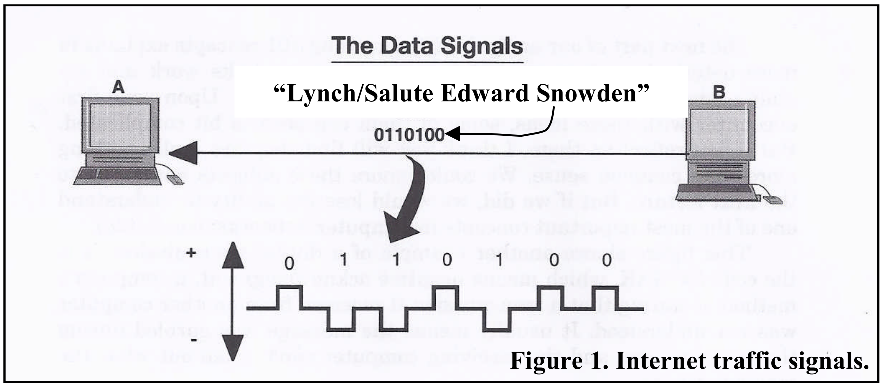

Figure 1. Internet traffic signals.

For this example, the email being sent from user B to user A, say, "Lynch/Salute Edward Snowden," is represented by electrical levels of voltage: a 0 is a positive voltage; a 1 is a

[1] Postal envelope in the reporter's thought cloud on the cover of this article is courtesy of Google.

negative voltage.[2] Signals sent through Wi-Fi, cable, copper wire, cellular, Bluetooth, satellite, and optical fiber use the basic scheme shown in Figure 1.[3]

Postal Service: The term *packet* refers to a digital envelope into which Internet traffic (of coded 0s and 1s) is placed. The packet contains the information needed to identify the receiver and sender of the traffic. It is similar to the "to" and "from" on a postal envelope, as seen in Figure 2. The top part of the address is "Bob" and the bottom part is "188 Anystreet, Anywhere, 88888." The cloud in the middle of this figure represents the postal service system that transports the mail from the sender to the receiver.

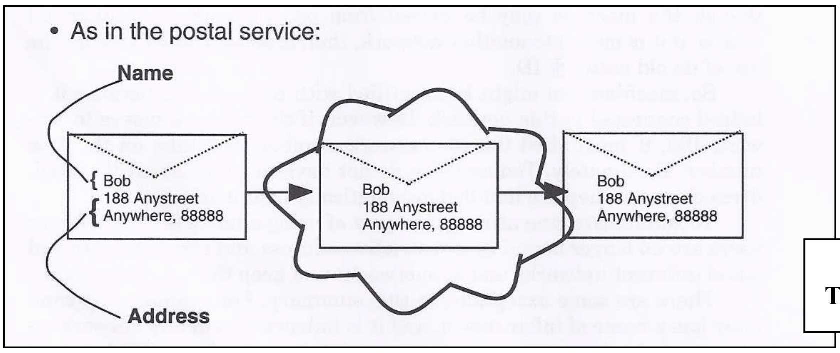

Figure 2.
The postal envelope.

As a general practice, the Postal Service does not care about the "Bob" part of the address. It uses the other parts to deliver the envelope to the receiver.[4] Furthermore, although Bob is a well-recognized name, this part of the envelope could be *anything*, such as "anon," or "machine," or "It does not matter."

Internet Service: The Internet uses concepts similar to the postal service. As part of its address, it also has a "Bob" type name. It is identified with various monikers, such as an email address, a uniform resource ID (URI), a uniform resource locator (URL), a Web site name, a Web address, and so on. Don't be concerned about these terms. They are not important for this report. Think of this name as an Internet identifier that performs the same function as "Bob." For purposes of comparison, I will also use the name "machine.com" as a generic handle for "Bob," as seen in Figure 3. They perform identical functions: *a handle to identify something that is independent of that something's location.*

[2] I am keeping the ideas of electrical current and phase out of this basic explanation. It is accurate as stated, but touches the surface of the subject.

[3] Contrary to popular myth, the world is not entirely "digital." On almost all media, the digital signals must be modulated onto analog frequencies. For this general discussion, just think digital codes as shown in Figure 1.

[4] I know of mail being delivered to a person with only, say, "Florine, Copperas Cove, Texas" on the envelope. I know, because I sent such a piece to my Aunt Florine, and it arrived intact at my aunt's mail box.

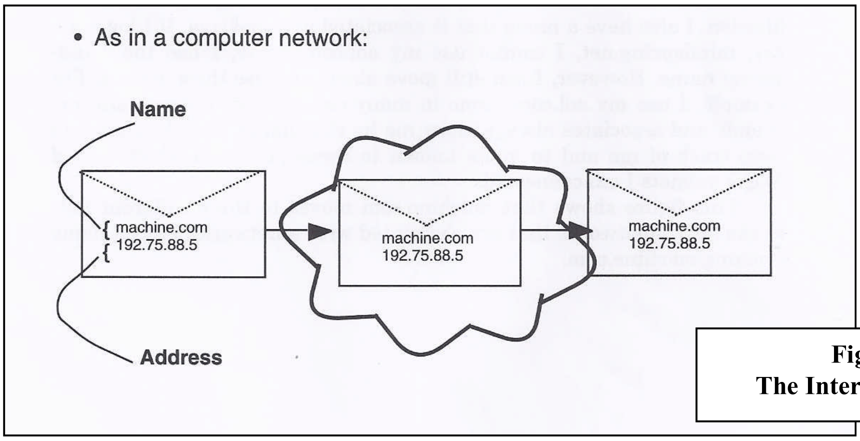

Figure 3.
The Internet envelope.

Like the postal service and "Bob," the Internet cannot use "machine.com" to deliver its traffic. Bob and machine.com have no geographical/physical significance. Consequently, the Internet once again mimics the postal service and uses another identifier for sending traffic to a recipient. It is called the IP address. It is similar in concept to "188 Anystreet, Anywhere, 88888" on a postal envelope: It is used to determine the physical location of the receiver of the traffic.

Figure 3 shows how the IP address is used in the Internet. The number "192.75.88.5" performs the same function in the Internet as "188 Anystreet, Anywhere, 88888" does in the postal service. It provides a means to deliver the traffic to a physical location; in this situation, the final intended recipient.[5]

It is likely you have seen Internet addresses on some of your computer screens or on printouts. The network technicians attempt to mask this address from your vision and your concern. That is one reason you hear many people say, "Send me your Internet address!" They do not mean the IP address, but your email "address," which is really a name. It is often an account name used by an Internet service provider, such as AOL and Google, to identify their customers.

To repeat, the so-called email address such as Bob.com or machine.com (or perhaps a more familiar format of UylessBlack@gmail.com) ***is not an address. It's a name.*** This point is emphasized because of later discussions about NSA's examination of citizens' names and addresses.

Translating Email "addresses" into IP Addresses

The Internet software and data bases are wonders unto themselves. Transparent to us, the Internet (and private networks that use Internet-type software) performs a service for Internet traffic like the postal service does for mail traffic: It keeps email and names independent of their location. The IP address of say,"192.75.88.5," is similar to "188 Anystreet, Anywhere, 88888." It is location-specific. So, our email (For that matter, Twitter, Facebook, etc.) traffic, if it uses the Internet, can be moved around anywhere in the world, and we do not have to obtain a new email "address"…which we know now is a name and not an address.

[5] In many parts of the Internet, the IP address is translated and mapped into different identifiers for purposes of efficiency.

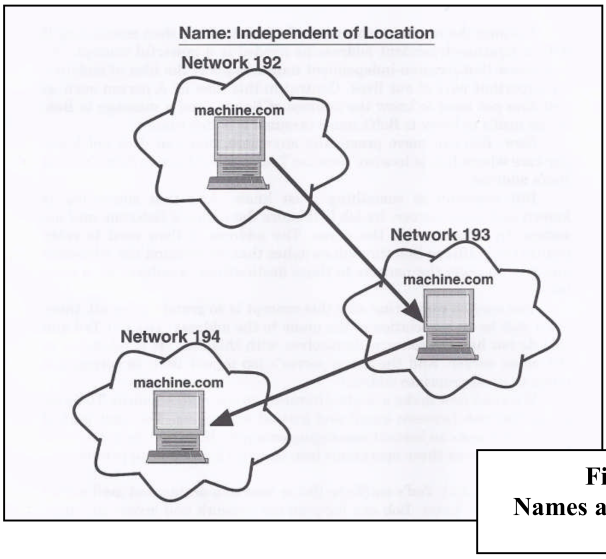

Figure 4.
Names and addresses.

For example, as Figure 4 illustrates, an email pertaining to machine.com can start in network 192 (say, Chicago), go through network 193 (say, Dallas), to end up in network 194 (say, Los Angeles). For that matter, machine.com can move to network 193 or 194 and not have to change machine.com to something else.

The same holds true for Bob. He can move from 188 Anystreet, Anywhere, 88888 to 199 Nostreet, Nowhere 99999, but he can still be called Bob.

Name Servers

When we send an email, Facebook photos, etc. (user content) to someone, it is not necessary to know their IP address. (Thank the Internet gods.) We need only know their email name, their account name, etc. Again, transparent to us, the system finds the IP address pertaining to the email or Facebook account and places this address into the packet for delivery. Figure 5 shows how this operation is performed.

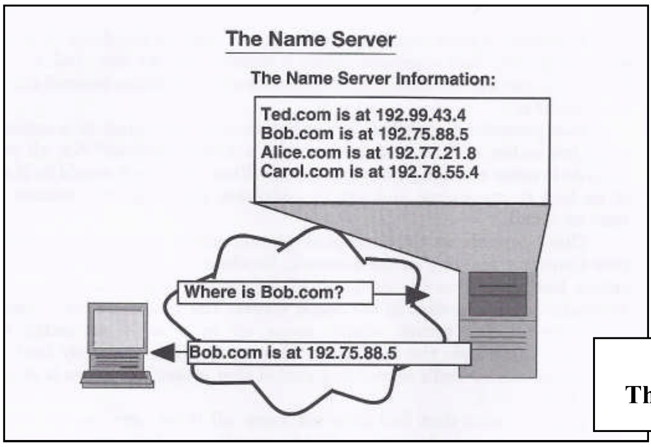
The Name Server
The Name Server Information:
Ted.com is at 192.99.43.4
Bob.com is at 192.75.88.5
Alice.com is at 192.77.21.8
Carol.com is at 192.78.55.4
Where is Bob.com?
Bob.com is at 192.75.88.5

Figure 5.
The name server.

Assuming the network is not congested and is thus responsive, in a matter of fractions of a second---after we hit the send key---a query is made to a system called a *name server*. This software might be located nearby or far away. (It might even be loaded into our computer.) Wherever it is, its job is to use, say, Bob.com to look up the IP address for Bob.com. In the example in Figure 5, it sends back a response of “Bob.com is at (address) 192.75.88.5.”

And in a matter of fractions of a second, again unbeknown to us, our machine assembles our message into a packet, places the IP address on the packet envelope (called a packet header) and sends to Bob, as seen in Figure 6.

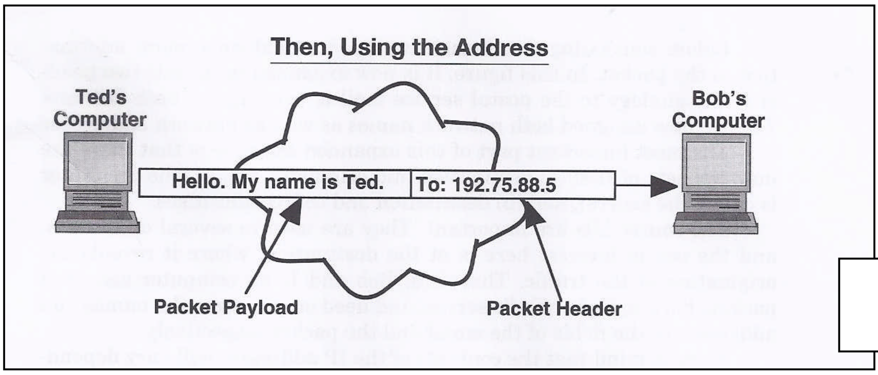

Figure 6.
The IP packet.

We are close to the point where we can return to the issue of NSA snooping and Internet privacy. Figure 7 will wrap-up this tutorial. The top part of Figure 7 (a) depicts the relationships of Internet names (such as account names, email names, Facebook names, etc.) and Internet addresses. Using the postal service analogy, the middle illustration shows how the user text is placed inside the envelope.

I have substituted machine.com with bob.com in order to simplify this and later discussions. They are identical in their function*: identify something that is independent of its physical address.*

Encapsulation

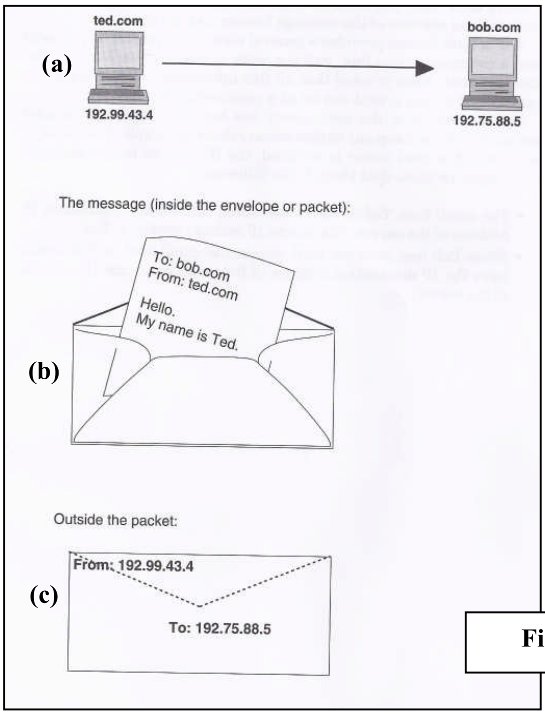

Figure 7. Encapsulation.

The middle illustration (b) of Figure 7 shows the user content (mail or email) that is to be placed inside the postal envelope (or the Internet packet). The bottom illustration (c) shows that the envelope or packet is "sealed." In Internet jargon, this idea is called *encapsulation*. The term refers to the condition of being enclosed, such as being inside a capsule.

Think of a medicine that is in capsule-form. The capsule (postal envelope or Internet packet) hides the medicine from its partaker. Granted, this imbiber can open the capsule and look at its contents. But like the postal service and the Internet, that is not the intent of encapsulation. The intent is to assume the contents of the capsule are not to be examined. After all, the information inside this capsule is not needed to relay its contents to the correct destination. That is the job of the information on the outside of the envelope (and the Internet packet header).

For this discussion, I emphasize a crucial point in the debate about privacy: In the bottom illustration, the envelope is sealed and cannot be examined by anyone except the intended receiver. The addresses on the envelope are used to identify the sender and receiver of the traffic.

Assuming the bottom illustration is an Internet packet, the same idea of privacy applies. Once the packet is assembled at the sender's device (computer, iPhone, etc.) the user traffic should remain opaque to all devices, servers, routers, tablets, phones, people---everything and everyone--- except Bob.

Yet, the Ted-to-Bob email "letter" may not be subject to this level of privacy, or it is certainly in danger of not being treated as such. But why not? Just because "Hello, My name is Ted." is represented in the digital world with electronic or optical images instead of pencil or ink images in the postal world, should that change our right to privacy of our correspondence?

I say no, and America's practice of the Bill of Rights says no.[6] As with the postal service, if Uncle Sam or Google wish to look inside this envelope, they should be required to obtain a court order to do so.

The Rub

Here's the rub: Digital data is just too easy to examine. Congress fell behind the power curve to curb this privacy invasion, so private enterprise started (a) examining and storing the entries on the envelope (an Internet packet), and in some situations, (b) began examining (inside the envelope) the text of the email. Before long, these organizations came to base much of their raison d'être for having access to more than the information on the outside of the envelope.

Think of the implications of this shift to the digital would in relation to our freedom of privacy and our right to be left alone. If the Internet world applied to the postal service world, anyone could go to my mailbox outside my home in Hayden, Idaho, pull out my mail, open the envelopes, and read the contents.

I am certain some of my readers will say no, that cannot be, it does not happen. But it does. Just ask Google. The more that is known about the contents of our communications with others, the more advertisements can be tailored to our tastes by the Googles of the world. And the more the Uncle Sams of the world can get into our privacy pockets.

Consider Figure 8. If the contents of our electronic letters can be read by others, the contents of our private souls can be exposed. I contend that privacy is indeed part of the human soul. Without privacy, our souls can be bared to the ridicule and exploitation of others.
Should we care? Do we harbor something in our lives that must be hidden from others? After all, with the opening of everyone's digital envelopes, the terrorist, the drug dealer, the pedophile, and other misfits of the world will be exposed. Their baring, their uncovering, will be for the betterment of society. Besides, we are clean of sin and crime. Take pictures of our homes. Read our mail. Tag our phone number to our personal names, to the street where we live.

I hope your side with me about the idea that privacy is a human sanctity. Without it, we lose a vital part of who we are and of what makes us different from others.

[6] The Constitution and Bill of Rights (as best I can read) do not address privacy of correspondence. But America's forefathers spoke of it and this sanctity of human discourse has long been embedded into our social and legal fabrics.

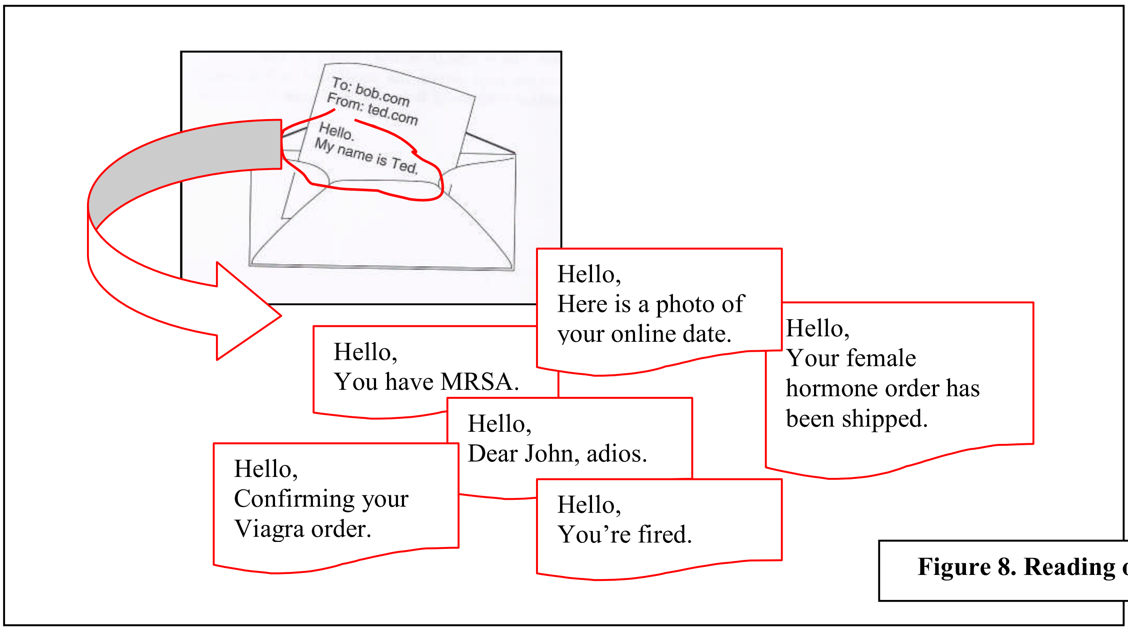
To: bob.com
From: ted.com
Hello.
My name is Ted.
Hello, Here is a photo of your online date.
Hello, You have MRSA.
Hello, Your female hormone order has been shipped.
Hello, Dear John, adios.
Hello, Confirming your Viagra order.
Hello, You're fired.

Figure 8. Reading our mail.

Another Rub

But the toothpaste is out of the tube. How can we go backward? How can a society recast the business models of Google and others that rely on our mail for their existence? How can a society deny the NSA access to the envelope and its contents when we are told if we do, we place ourselves at the mercy of terrorists? Just because our letters are now electronic, have things changed so much to render privacy irrelevant?

These questions should be posed to the lawmakers in Washington. Perhaps they can put the toothpaste into the tube that they should have sealed many years ago. But then, who knew the vendors of wares would take over the Internet?

Your on the Street Reporter