Have you been Reading my Email?

Have You Been Reading My Mail?[1]
Part One

Yesterday, you went to the mailbox to retrieve your letters, bills, and advertisements. There, you were surprised to find your neighbor as well as a stranger examining your envelopes. They also opened several of the envelopes and read the contents inside them.

Your reaction? I will not venture a guess, as this is a family newspaper, but I would speculate it would not be one of acceptance. Yet this situation is identical to what is happening to our Internet correspondence, our email. To frame the issue, which I hope will raise your concern about privacy in the Internet, I will start with two questions pertaining to postal service mail:

- Should anyone but the recipient of a letter be allowed to *read and record* the information on the envelope?
- Should anyone but the recipient of this envelope be allowed to *read and record* the information in the letter that was placed inside the envelope?

I suspect your answer is no to both questions. If so, next question: Why should we relinquish this right of privacy because our letters are written in electronic images instead of ink or pencil?

Some will answer: The Internet is not the U.S. Postal Service. True, but the Internet was founded courtesy of the American taxpayer and the U.S. government. Furthermore, at the rate citizens are moving from conventional mail to electronic mail, it is reasonable to assume Internet mail will supplant U.S. mail as the dominant medium for sending and receiving correspondence.

Given this trend, by calling our letter "email" instead of "mail," and using a salutation of "Hi" instead of "Dear," does that relinquish our rights to seclusion? Why should this private space to ourselves and those to whom we send correspondence suddenly become space for everyone to share?

By changing the delivery mechanism for our message---from the postal service to the Internet--- our envelopes can be opened and our letters read. Not just by Uncle Sam's NSA. Not just by Google. Eventually, by *anyone*. Think about that idea for a minute or two, because that is where we are heading.

Last question, what has happened, in only thirty years or so, for our society to reach a point in which the CEO of Google states:

> …after privacy concerns were raised…Eric Schmidt, declared: **"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.**[2]

I place Mr. Schmidt's quote in bold type because his assertion is straight out of an Orwellian scenario. Eric Schmidt is the Chief Executive Officer of the most powerful and influential Internet-based company on earth.

---

[1] This piece was formatted for publication in the *Coeur d' Alene Press*. Envelope in thought cloud on cover is courtesy of Google

[2] "Will We Ever Get Strong Internet Privacy Rules?" *Time*, March 5, 2012.
Also see: Cade, Metz (December 7, 2009). "Google chief: Only miscreants worry about net privacy," *The Register*.

He implies nothing is out of bounds to be examined: Your letter to your siblings about your parents' failing health. Your debate with the IRS about your taxes. A credit card transaction. Your "Dear John" to Joan. Joan's "Dear John" to you.

According to Schmidt, the Internet has altered the game. Cyberspace, because it is no longer a pen-and-ink world, renders our right to privacy irrelevant. After all, we have nothing to hide. Nothing to hide except one of the most treasured aspects of our nature: our privacy, our right to be left alone.

On the August 24 *60 Minutes* program an Internet vendor said, "The Internet is an advertising medium." In fewer than three decades, the Internet has evolved from a network dedicated to the exchange of personal electronic mail and small files to one where this person declares it to be dedicated to selling various wares. How are these wares sold? By the sellers increasingly obtaining more-and-more personal information about you and me.

The second article in this series will offer some ideas on how to seal your electronic email envelope. The suggestions will not protect the privacy of the addresses on the outside of the envelope, nor will they necessarily stem the tide of Internet advertisements. But they will offer ways to protect the contents inside the envelope: our personal correspondence.

By the way, don't throw away your postage stamps. They may come in handy

Have You Been Reading My Mail?
Part Two

In the first article of this series, I made the well-known claim that our Internet mail is not private. Our electronic letters can be read by anyone who has a smattering of knowledge about Internet email.

Given that electronic mail is supplanting hard copy mail, how can we American citizens go about living our personal and professional lives under the cloud of having forsaken privacy? The Internet vendors tell us we should not be using the Internet if we have something to hide.

I disagree. Most of us use the Internet to exchange harmless, yet sometimes sensitive letters with our loved ones and friends. They are often personal and private. If they are exposed, they will not do us under, but why should they be exposed in the first place?

The Internet vendors say our correspondence needs to be examined in order for their sales outlets to "profile" us---to find our tastes and distastes---for their targeted ads. Imagine! We have become marketing guinea pigs for Internet's Madison Avenue.

Perhaps this exposure of our personal life could be considered harmless. After all, why should we care if a health monitoring website learns we have recently been diagnosed with cancer, and we might be denied care or pay more for insurance? Why should we be concerned if neighbor Joe knows our spouse has left us and taken our credit cards in the process?

I wager I am a preacher talking to a concerned congregation, because I sense all of us care. The Internet was conceived as a network for personal communications, not as a network for commercial advertisements. I am not opposed to money-making billboards. One of my former companies was built around advertising, but I did not check-out the religious, political, and sexual preferences of my advertising targets---as is being done today.

What can we do to gain back our privacy in a system that is rendering U.S. mail moot? In view of Facebook, YouTube, and Linkedin onslaughts, how can we keep the valued American treasure of privacy intact?

Answer: We cannot. The gate has long been opened, and the Internet advertiser cows are in the pasture, feeding on the long grass of information about you and me.

In hindsight, the Internet email envelope should have been given the same sanctity as a U.S. mail envelope. But no one in the early times of the Internet (including this writer) foresaw how the network would evolve.

A Commercial and Social Problem

I doubt the clock will be rolled back to treat email with the same respect for privacy as regular mail. The lobbyists for keeping the Internet as an advertising and data-retrieving medium are too powerful for Washington to muster the political will to make amends, even if it had the constitutional authority to do so. Thus, unless the Supreme Court takes the matter into its hands, it is reasonable to predict that the Internet will evolve to a point where very little information is treated as private.

However, all is not lost. I conclude this article with some good news: simple actions that Internet end-users can carry-out to take-back some of their privacy.

Encrypting Emails and Smartphone Traffic

These two articles have been devoted to a specific kind of Internet end-user traffic: email. This emphasis continues, but I interject the idea that similar privacy protection can be obtained with other traffic as well, such as voice traffic.

An Internet end-user does have an effective line of defense (as of this writing): The use of encryption applications (apps) allows the communicating parties to scramble (encrypt) their correspondence. Unless Uncle Sam or sophisticated hackers move to the next level of breaking the codes of these apps (which they are working on), our electronic mails can once again have their envelopes sealed. For example, Google Message Encryption (GME) enables end-users to secure their email by using a Google security package.

To conclude this series, I take us one step further than what companies such as Google offer in protecting privacy. These systems protect our privacy while our email is in the Internet. They do not protect our privacy after the emails have been unscrambled and placed on our computer.

If we are concerned about the privacy of the files stored on our machine, it is a simple matter to use another package to scramble this data. In this way, this information will be known only to us and anyone with whom we wish to share the "key" to "unlock" this information. For example, the widely-used Microsoft WORD has an easy-to-use encryption option that allows a user to scramble any WORD document.

As mentioned, the same kinds of security packages are available to end-users who use smartphones. They, too have encryption packages.

If you are not using these security services, it can only be assumed you do not mind if others know about your written and spoken communications. On the other hand, if you do care but you continue to ignore them, you have abandoned Benjamin Franklin's advice: Be aware that *distrust and caution are the parents of security*. …and privacy.

