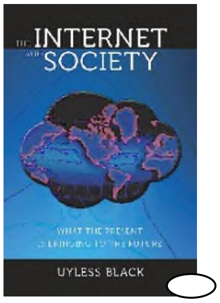


Your on the Street Reporter

Uyless Black

The Internet and You

(Volume II of a series of newspaper articles)

The Internet and You

COEUR d'ALENE
PRESS

These articles were written for the *Coeur d' Alene Press*, a paper operating out of Coeur d' Alene, Idaho. Their contents (covered in more detail) can also be found in a book that will be published in the spring of 2016 titled *The Internet and Society: What the Present is bringing to the Future*.

They are arranged in two separate volumes to ease in downloading. Nonetheless, each article is short, fewer than 1000 words. The scanning of the newspaper articles into WORD and PDF formats created more (invisible) overhead. I make these comments to assure you each article will be a short read…which I hope will encourage you to read them!

I look forward to your comments. Send to UBlack7510@aol.com.

COEUR d'ALENE
PRESS
SERVING KOOTENAI COUNTY SINCE 1892.
www.cdapress.com

Monday
January 11, 2016

The Internet: Watching government surveillance

By UYLESS BLACK
Special to The Press

After the 9/11 attacks, America's citizenry and its intelligence community developed a fear of what might follow. To compound citizens' fears, the crumbling to earth of the Twin Towers also crumbled many peoples' faith in America's intelligence community. Critics claim Uncle Sam's intelligence agencies failed to do their jobs. In response, the NSA, FBI, DIA, and CIA claim if they only had access to more data, the Twin Towers would still be standing.

The PATRIOT Act

More data, more information, became the mantra for the solution to the terrorist problem. One result was the passing of the USA PATRIOT Act, signed into law by George W. Bush on Oct. 26, 2001. NSA, acting on the laws of the PATRIOT Act, put in place a surveillance system that captured "every possible scrap of information," what General Keith Alexander, the agency's former head, called "the whole haystack."

Black

These acts and rulings empowered the government

See UYLESS, A3

The Internet and you

- **Jan. 4:** Intrusive advertisements
- **Jan. 5:** Net neutrality
- **Jan. 6:** Protecting user content
- **Jan. 7:** Twitter and literacy
- **Jan. 8:** Big data and metadata
- **TODAY:** Government surveillance
- **Tuesday:** Commercial surveillance
- **Wednesday:** Hard copy and concrete
- **Thursday:** All about clouds
- **Friday:** Who controls the Internet?

UYLESS

from A1

to direct any American company or individual to disclose records of national security interests (as determined by FISA, the Foreign Intelligence Surveillance court). In addition, NSA has used these tools as the basis in its metadata gathering programs for the FBI's law enforcement actions.

The New America Foundation, a liberal to middle-of-the-road think tank, performed an analysis of the methods used to detect terror suspects. Here is a synopsis of this study, which can be found at http://natsec.newamerica.net/nsa/analysis:

*The Foundation asserts the NSA's bulk surveillance of phone and email communications records is having no effect on keeping Americans significantly safer. The organization states NSA's claims of the program being effective are "overblown and even misleading." Gen. Keith B. Alexander eventually conceded that the program had uncovered one or two plots.

*An analysis of 225 individuals charged in the United States with an act of terrorism since 9/11 reveals that traditional investigative methods (use of informants, tips from local communities, targeted intelligence operations) provided the foot in the door that led to these indictments.

*The contribution of NSA's metadata surveillance programs to these cases was at most 1.8 percent of these cases.

Taking a look on the other side of the fence, do these admittedly small figures reflect an ineffective program? Was the 1.8 percent of the people in the sample planning on leveling the White House? *It is not just the quantity of the traps that matters, it is the quality of what was trapped that is more important.*

The men and women in the American intelligence community have the best interests of America at heart. However, the very nature of their jobs can lead them to over-react. (I can attest to this tendency during my time as a U.S. Navy officer assigned to the Defense Intelligence Agency.) It is human nature. The danger of this situation is that secret over-reach tends to build on itself because it lacks restraints. (Congressional oversight committees have been, charitably speaking, lax in their oversight.)

USA Freedom Act

Due to concern and complaints about the PATRIOT act (and its illegal misuse), Congress passed the USA Freedom Act in 2015. This act establishes a new process for the FBI and NSA to follow in obtaining permission from the FISA court for examining records gathered by American wireless and wire-based telephone companies (and by inference, Internet traffic as well).

In contrast to the PATRIOT Act, which led to warrantless searches of records that were stored at NSA, the USA Freedom Act requires the FBI and NSA to do their probing on a case-by-case basis. In addition, these records will no longer be stored at NSA. (What happens to the massive NSA Utah facility?) They will be stored at companies' sites. The act permits "the government to require the prompt production of such records," and to compensate any party for expenses incurred for producing the records.

As with the PATRIOT Act, the USA Freedom Act's intent is to obtain foreign information "to protect against international terrorism or clandestine activities." As well, the collection and examination of user content in traffic is not allowed; seemingly, only metadata. However, the FBI is still allowed to submit an application to the FISA court to obtain "tangible things" such as business records, books, records, "and other items." The "and other items" phrase is broad enough to include Internet traffic and user content.

More Openness

A substantial part of the Freedom Act is devoted to the process of obtaining and examining information to be subject to less secrecy; that is, more openness to Congress.

In addition, the act requires the Director of National Intelligence to make available publicly the total number of searches conducted during a preceding 12-month period. As well, an Internet website must be created that reflects the number of FISA court requests denied (or approved) during this time.

This approach, using America's legacy of court-approved "wire tapping," is a healthy change from the PATRIOT Act. But we should keep in mind that after 9/11, America's citizens and its intelligence community were caught-up in a vortex of uncertainty and alarm. Only in hindsight do we have foresight.

The Cybersecurity Information Sharing Act

The Cybersecurity Information Sharing Act (CISA), passed by the Senate on Oct. 28, 2015, is intended to facilitate the sharing of information about Internet security threats between U.S. government agencies (national, state, and local) and private enterprise. As of this writing, it is too soon to know the consequences of this law. The details have not yet been filled in.

Also, it remains to be seen how this law will affect the USA Freedom Act, but this writer believes it might compromise aspects of the "Freedom" law. That said, CISA does require the stripping of personal information when data are exchanged between various parties. Metadata is the focus of attention.

Privacy advocates worry that the act does not establish how the information will be controlled. Proponents of the act claim that CISA will help prevent corporate data breaches by allowing companies to share cybersecurity threat data with security agencies such as the Department of Homeland Security, the FBI, and NSA. The Wall Street Journal claims the law will combat cyber threats.

The interested reader can follow the maturation and implementation of both laws on the Internet. I will post updates to this information at Blog.UylessBlack.com. Scroll down to Series #26 and click on the link, "Epilogues to The Internet and Society." (Thus far, there are no updates to post.)

The U.S. government surveillance operations are controversial, often raising political blue or red flags. U.S. businesses stand to lose billions of dollars in revenue because other countries (even the EU) are passing laws forbidding their citizens' data to be sent across country borders. The Internet may be divided in fiefdoms as countries are forced to balkanize their parts of the Internet. We return to this subject in the last article of this series.

Uyless Black is an award-winning author who has written 40 books on a variety of subjects. His latest book is titled "2084 and Beyond," a work on the origins and consequences of human aggression. He resides in Coeur d'Alene.

COEUR d'ALENE
PRESS
SERVING KOOTENAI COUNTY SINCE 1892
www.cdapress.com

Tuesday
January 12, 2016

The Internet: Watching commercial surveillance

By UYLESS BLACK
Special to The Press

At the rate citizens are moving from conventional mail to electronic mail, texting, and instant messaging, it is reasonable to assume Internet correspondence will supplant postal mail as the dominant medium for sending and receiving correspondence.

Given this trend, by calling our correspondence "email" instead of "mail," and using a salutation of "Hi" instead of "Dear," does that relinquish citizens' rights to seclusion from the world's eyes? Why should this private space to ourselves and with those whom we exchange messages suddenly become space for everyone to examine?

Black

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 or FBI (who now claim they examine only metadata, unless in possession of a court order). Not just by Google. Eventually, by anyone. Google itself has stated it has read user content.

(For clarification, I exclude the social media databases in this discussion. Anything we place on Facebook, YouTube, and similar websites is fair game for anyone to use: That is the price paid for telling the world about ourselves. In a nutshell, we asked for it.)

See BLACK, A10

The Internet and you

Jan. 4: Intrusive advertisements
Jan. 5: Net neutrality
Jan. 6: Protecting user content
Jan. 7: Twitter and literacy
Jan. 8: Big data and metadata
Monday: Government surveillance
TODAY: Commercial surveillance
Wednesday: Hard copy and concrete
Thursday: All about clouds
Friday: Who controls the Internet?

Fortunately, we learned in this series that we can protect our privacy by encrypting our content. But that does not include having our lives involuntarily exposed through online government and commercial files.

The last question: What has happened, in only 30 years or so, for our society to reach a point in which the chief executive officer 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."**

I place Mr. Schmidt's quote in bold type because his assertion reflects an Orwellian mentality. Eric Schmidt is the head of the most powerful and influential Internet-based company on Earth. 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 Joan" to Joan or Joan's "Dear John" to you. And for what purpose does Mr. Schmidt use this information? Among others: targeted advertisements! Our personal and professional lives have become input into a digital Madison Avenue.

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 human nature: privacy, the right to be left alone.

I have one piece of advice for Mr. Schmidt: Don't forget to take off your Google glasses when you are having sex. After all, you have nothing to hide as those packets displaying your sexual exploits find their way into the Internet.

Data Brokers

The Internet has become so commercialized that companies exist for the sole purpose of mining databases, such as government files and social media. These organizations apply big-meta technology to that information, and sell it to others. One company states it has collected 1.1 billion "cookies." It is information that shows a user's browsing preferences. It is metadata that reveals much about the habits and behavior of a person or organization. This company also states it has more than 200 million mobile phone metadata records.

Let us all take a bow! You and I are the source of those Internet companies' wealth.

Opening Envelopes

In an ideal environment for the end-users, after an Internet packet is assembled at the sender's device and sent, the user data will remain hidden to all devices, servers, routers, tablets, phones, people — everything and everyone — except the end-receiver(s) of the traffic.

Yet our traffic may not be subject to this level of privacy. As the slang goes, here's the rub: Digital data is just too easy to examine, almost effortless. Congress fell behind the power curve to curb this privacy invasion, so private enterprise started (a) examining and storing the metadata entries on the envelope (an Internet packet), and in some situations, (b) began examining (inside the envelope) the contents of the end-user traffic.

Before long, these organizations came to base their raison d'être for having access to users' Internet traffic. We can at least bask in the knowledge that our data has made a lot of Internet vendors very wealthy.

Is Privacy Important?

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 might 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.

In closing this part of the series, I hope readers will rally to the idea that privacy is a human sanctity. Without it, we lose a vital part of who we are.

I have had numerous discussions with friends and colleagues who inform me that I should not use the Internet for sensitive correspondence. I do not consider accessing my bank online to enquire about my balances to be sensitive correspondence. Nor do I think my doctor should be hesitant in sending me a text about the results of my PSA test.

On and on we could go, but my single answer to my critics is a question, "Fine, but what happens when the only way to correspond with my bank or doctor is electronically?" Conventional mail will go the way of the telegraph. It is only a matter of time. What then?

Uyless Black is an award-winning author who has written 40 books on a variety of subjects. His latest book is titled "2084 and Beyond," a work on the origins and consequences of human aggression. He resides in Coeur d'Alene.

COEUR d'ALENE PRESS
SERVING KOOTENAI COUNTY SINCE 1892
www.cdapress.com

Wednesday
January 13, 2016

The Internet: Eroding hard copy and concret

By UYLESS BLACK
Special to The Press

With the increased use of the Internet for the transport of email, text, and instant messages, it is logical to assume there would be an associated decrease in the transport of hard copy mail. Likewise, the same idea would hold for an increase in online shopping and a decrease in business at street stores, as well as a surge in Internet traffic and a decline in hard copy news circulations. These are indeed the trends, as discussed in this article. If these trends continue, the world's societies and how people spend time will be altered significantly.

Black

This article uses Cisco's study about the future of different types of Internet traffic volume. I thank Cisco for this source of information. You can obtain more details at:

http://techreport.com/news/28341/cisco-says-video-will-drive-massive-growth-in-internet-traffic.

Postal Service Traffic

Given the cost and time to send a first class letter, especially in comparison to send-

See BLACK, A2

The Internet and you

Jan. 4: Intrusive advertisements
Jan. 5: Net neutrality
Jan. 6: Protecting user content
Jan. 7: Twitter and literacy
Jan. 8: Big data and metadata
Monday: Government surveilla
Tuesday: Commercial surveilla
TODAY: Hard copy and concret
Thursday: All about clouds
Friday: Who controls the Intern

BLACK

from A1

ing an Internet email or text message, it comes as no surprise that the U.S. Postal Service is shutting down some of its retail offices and processing centers. An original announcement declared 672 offices (of 32,622) would be closed, but that figure was cut back because of public and political blowback.

The United States is not the only country experiencing this decrease. Postal services in many parts of the world find themselves in an upward pricing/downward volume spiral. As they experience a smaller customer base, they must raise the prices on their stamps to make up for the difference in revenue. This action leads to more customers leaving their fold, which requires raising the price of postage stamps to cover the decreased customer base.

As noted in an earlier article, to add fuel to the fire that is burning up the first-class mail industry, many Internet vendors provide a customer with the ability to sign an Internet document, a process known as a digital signature. In the past, electronic correspondence has been handicapped by the lack of a feature to validate a piece of correspondence and its originator. It is now possible to authenticate Internet correspondence with a digital signature. The technology is widely available and can serve as a replacement to registered mail as well as signatures certified by a public notary (depending on local laws).

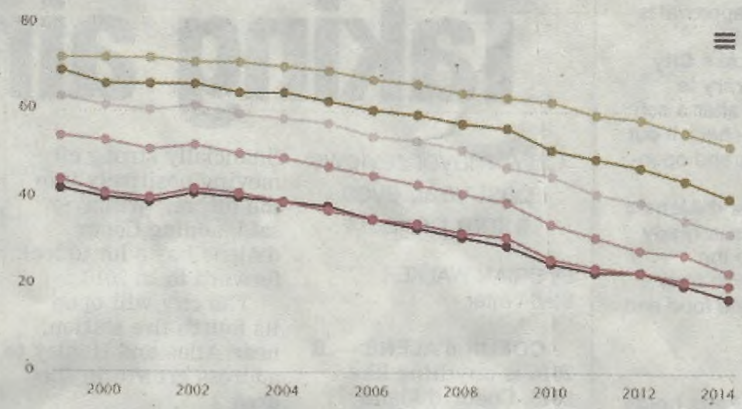
Street Retail Stores

As the store closed its doors for business, the manager of a failed retail store succinctly summed the situation, "The staff at Jessops would like to thank you for shopping with Amazon." This is not to say the entire retail store industry is going the way of this store, as several countries (such as China) continue to expand on-the-street-shopping. However, given the increase in online shopping, along with the speed and ease of using commercial delivery systems, the conventional retail business does not look promising.

The overhead of street stores cannot compete with their online counterparts. The online retailers have no elaborate store facades or interiors to maintain. The sales staff is usually composed of banks of computer servers. They have few or no people with union or pay issues. If the user screen interfaces are well designed, online shopping can be a pleasant and rewarding experience.

Unless resolved by the courts or Congress, some states will continue to pay no taxes for Internet sales. The legislatively ordained tax exemption granted to online retailers places the street vendors in an even more untenable position in relation to their online competitors. Additionally, it denies local, state, and national governments income to support public services. These bodies lose the taxes traditionally gained from street sales, but are not compensated by the migration of these sales to the online world.

The Internet and Society: What the Present is Bringing to the Future



Video Traffic: The Game-Changer

Internet video traffic will account for 80 percent of the total Internet traffic by 2019. Gaming downloads are increasing in volume, as end-users migrate to the Internet for entertainment. Games usually consume considerable bandwidth, as they have elaborate interactive graphics for their displays.

Unless the cable and satellite TV industries change their offerings and pricings, they are destined to experience a loss of customers to the mobile video and Internet video industries. This trend might continue regardless of what Comcast, Time-Warner, Direct TV, and DISH do — unless they get into the mobile and Internet video market. Customers have had it with purchasing packages containing mostly programs for which they pay but never watch. In the long run, the current cable TV and satellite TV models make no sense.

This situation is called "cord cutting" in which Cisco states, "Traditional and subscription television viewing is increasingly being supplanted by other means of video viewing, such as [Internet] and mobile video."

Hard Copy News

The traditional newspaper business has been in freefall for several years. A study by the American Enterprise Institute (AEI) states print advertisement revenues are the lowest they have been since 1950. As part of the AEI study, the figure in this article shows that the readership of daily newspapers in the United States has been in decline for over a decade.

The information shown in the above figure likely comes as no surprise to the reader. Habits die hard. Older people are accustomed to getting their news from conventional newspapers (and television). The younger generations are more in tune with online news. I was surprised by the data in this figure, as I had thought newspaper readership had declined more than is shown in this study. Perhaps there is hope for a literate world after all.

The good news to those who treasure the written word and conscientious journalism is that several responsible newspapers and magazines are still plying their trade. Some are making the transition to the online, digital world, although they are struggling to bring in advertisement revenue. The newspaper that is publishing this series, the *Coeur d'Alene Press*, has installed a state-of-the-art online system. (I was not paid for this endorsement.)

The cities of today, with their downtown shopping areas, the hustle and bustle of the crowds, the sometimes frustrating vitality of congested sidewalks and freeways, cannot be replaced by the lone shopper sitting at his/her home of office looking for wares that are offered in the stores.

At least, that has been my contention for most of my life. But I could be wrong. Some of my colleagues told me that the Millennial generation's preference for social networking includes a penchant for online shopping. After all, they have been conditioned for stand-alone interactions for many of their waking hours.

Notwithstanding these trends, how about that refreshing lunch during a shopping trip, perhaps the afternoon drink before heading home? Amazon is working on the answer: Drone-delivered dinners and cocktails to our front doors.

Uyless Black is an award-winning author who has written 40 books on a variety of subjects. His latest book is titled "2084 and Beyond," a work on the origins and consequences of human aggression. He resides in Coeur d'Alene.

COEUR d'ALENE
PRESS
SERVING KOOTENAI COUNTY SINCE 1892
www.cdapress.com

Thursday
January 14, 2016

The Internet: Clouds — servers or oligarchs?

By UYLESS BLACK
Special to The Press

Cloud computing is being touted by cloud vendors as the best way for Internet users to back up their files as well as receive services, such as software support, including automatic updates to their applications. These users are individuals as well as small and large organizations. Some cloud vendors offer to augment, if not replace, a company's data center with their clouds' data centers. Typical cloud services include:

Black

• Creation of apps: Tailor-made applications that run on different systems.

The Internet and you

Jan. 4: Intrusive advertisements
Jan. 5: Net neutrality
Jan. 6: Protecting user content
Jan. 7: Twitter and literacy
Jan. 8: Big data and metadata
Monday: Government surveillance
Tuesday: Commercial surveillance
Wednesday: Hard copy and concrete
TODAY: All about clouds
Friday: Who controls the Internet?

• User database and software support: Backup and security features.

• Virtual machines: Obtaining additional computing power from thousands of computers that belong to a cloud vendor.

• Security and privacy Most commercial clouds offer the Advanced Encryption Standard, and multistep encryption, discussed in Article 3.

• Expertise: A cloud business customer need not hire a full staff of experts, which can be expensive.

Caveat Emptor

Given these attractive features, one might wonder why all users do not close down their data centers and migrate to a commercial cloud? Or why Uyless Black does not turn over his family photographs to a cloud? The most common answer is loss of control of one of the most valuable resources an institution or individual possesses: data and software.

Many companies and individuals do not trust their automated systems to another party, regardless of how competent that party may be. The situation is complicated by legal problems dealing with the potential loss of privacy because of a security breach.

In addition, there is the issue of cost. Referring to Microsoft's Azure, its Software as a Service (SaaS) feature rents Microsoft software to its cloud customers. I emphasize the word rent, instead of purchase. It is no surprise that software vendors are migrating toward preventing a potential customer from buying a package.

In the past, a purchased package could be used for years without paying any more beyond the purchase price. The vendor stands to make more money by renting its software than by selling it. In the long run, the customer ends up paying more.

In the future, it is safe to state that users will no longer be able to purchase most software packages. The programs will be rented and downloaded from the vendor's cloud. The future computers and mobile devices will be empty hulls of hardware, with the rented software controlled by the cloud.

If an individual user only needs hand-holding and occasional help, an effective alternative to a cloud is to pay a vendor a modest annual fee for near-immediate access to competent technical help.

UYLESS BLACK

While I was writing this series, I received this email from one of my colleagues:

When I logged on this morning, a banner of words crossed my screen, I paraphrase: We are excited to show you new features that you will love. I could not move on. I waited, waited, waited, so I pressed escape—nothing. I became frustrated, as I had not expected this interruption, and I had other time commitments. I did Ctrl alt delete [a Windows method to be released from a session], then went back to my screen. Finally, the sentence disappeared, with the note, new applications have been installed, but no information on what, no request to wait to install, just a takeover of my computer. Then, small notes appeared, sliding out from the right side, giving new things I could expect, which I did not want.

Unless Uncle Sam decrees some kind of control over these sorts of software dictatorships, my friend's experience will become the tip of the iceberg. I am consistently reluctant to have government's heavy hand step in. But what could be heavier than the experience my colleague had?

Oligarchs and Government Oversight

As a retired owner of three telecommunications firms, I sometimes grew leery of FCC's regulatory hand. Nonetheless, I favor the FCC rulings on Net neutrality, discussed in Article 2 of this series. Internet vendors will not police themselves. After all, they are capitalistic enterprises. A recent case in Texas bears examination (this is a partial quote from a news release issued May 12, 2015 (italics are mine)):

AUSTIN - Attorney General Ken Paxton today announced that the Texas Attorney General's Consumer Protection Division—along with the Attorneys General of the other 49 States and the District of Columbia, and the federal government—reached settlements with Sprint Corporation ("Sprint") and Cellco Partnership d/b/a Verizon Wireless ("Verizon") that resolve charges of "mobile cramming" against the companies. The settlements include $158 million in payments, and resolve allegations that Sprint and Verizon *placed charges for third-party services on consumers' mobile telephone bills that were not authorized by the consumers, a practice known as "cramming."*

***

Consumers who have been "crammed" often have charges, typically $9.99 per month, for "premium" text message subscription services *that the consumers have never heard of or asked for, covering such topics as horoscopes, trivia, and sports scores.*

What to do?

Cloud computing is seen by many as the dominant way the Internet will be used in the future. There is no question commercial clouds offer fine and often extraordinary services to their customers. Nonetheless, the evolution toward end-users losing control of their data and software cannot be taken lightly.

As clouds take over, user competence and expertise diminish as more and more operations are removed from end-user machines and moved to clouds. This situation has the potential to form a risky cycle: As the end-user relinquishes responsibility and knowledge of his/her computing world, the cloud becomes more powerful and knowing, which leads to further degradation of the end-user's control and knowledge.

I do not intend to come across as a Chicken Little shouting, "The sky is falling." However, it is possible for the cloud vendors to become Internet oligarchs. I reluctantly concede that the FCC should remain alert to protect the Internet end-user from any large and powerful company abusing its position, such as the example in Texas demonstrated.

As well, I await the likely fervent counter-claims from the commercial cloud vendors. Before they protest, I ask them to re-read the findings of 50 states, the federal government, and my friend, described above. Granted they aren't Volkswagen, but their behavior does not augur well for giving commercial clouds the license to do as they please..

If an individual user only needs hand-holding and occasional help, an effective alternative to a cloud is to pay a vendor a modest annual fee for near-immediate access to competent technical help. I subscribe to Microsoft and Apple technical support services, as well as Best Buy's Geek Squad. All are outstanding and reasonable in cost in relation to the amount of time and expertise they spend on my problems.

One last idea: If you use vendor-specific help desks, make certain you instruct them not to install something that favors their system over that of a competitor's. For example, changing your default Internet browser from, say, Google's Chrome, to Microsoft's Bing.

Uyless Black is an award-winning author who has written 40 books on a variety of subjects. His latest book is titled "2084 and Beyond," a work on the origins and consequences of human aggression. He resides in Coeur d'Alene.

COEUR d'ALENE
PRESS
SERVING KOOTENAI COUNTY SINCE 1892
www.cdapress.com

Friday
January 15, 2016

Who controls the Internet?

By UYLESS BLACK
Special to The Press

Black

For the past two weeks, this series has focused on current Internet issues, as outlined in the list shown in this article. One issue, the performance of America's broadband carrier industry, was covered in an earlier series (July 31 – December 15, 2014) and bears reviewing and updating. A New York Times study claims the U.S. still lags behind other countries in performance/cost operations. Some examples are shown in the figure that accompanies this article (page A8).

In several American cities, conventional broadband carriers are not providing these high-capacity services. According to the Times study, Google provides this service in Kansas City, and publicly owned networks provide them in Lafayette, Chattanooga, and Bristol.

See BLACK, A8

The Internet and you

Jan. 4: Intrusive advertisements
Jan. 5: Net neutrality
Jan. 6: Protecting user content
Jan. 7: Twitter and literacy
Jan. 8: Big data and metadata
Monday: Government surveillance
Tuesday: Commercial surveillance
Wednesday: Hard copy and concrete
Thursday: All about clouds
TODAY: Who controls the Internet?

The broadband carrier industry cites its own studies that offer counter-claims, once again leading to the old saw, "Where one stands depends on where one sits." In my travels last year across various American cities, I can report (anecdotally) that the U.S. broadband carrier industry performance is improving, but it is still spotty.

I recommend you contact your local broadband carrier to discuss performance and inquire if you are being given the full bandwidth that is available. A couple years ago, I did the same, and overnight my throughput doubled (for the technicians reading this article: from DS-1 speeds to DS-3 speeds, yet still very slow).

For other issues discussed in this series, we should be resigned to the fact that Big Data and metadata (bigmeta) are not going away. They will become more sophisticated in gleaning information from users' Internet and cellphone traffic.

However, we should not be resigned to any party examining our private mail, text, and phone calls unless it is done through a court order. Conventional postal services will continue to decline and electronic correspondence will largely supplant the post office. Therefore, we users should insist on having privacy for what we wish to be private.

To that end, users should take time to encrypt sensitive data (as well as to communicate with congressional representatives and the FCC about the issue of privacy). Individuals and organizations need not learn the hard way by having their databases and software compromised.

Screen Control Equals Control of the User

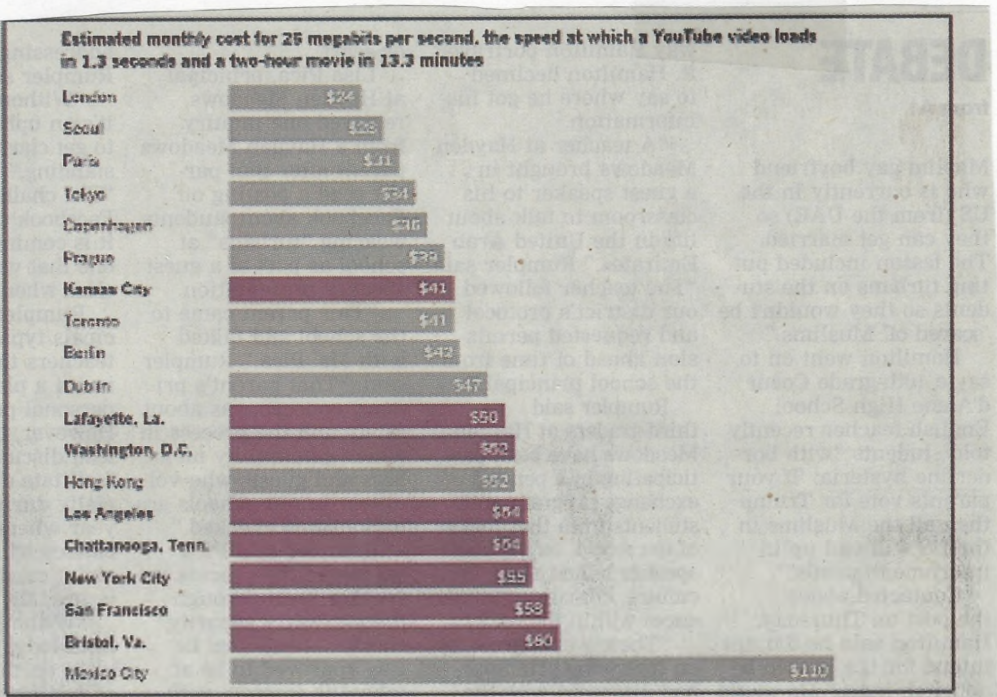
Who is to control what appears on the screens of the user's machine? The answer to this question affects how all users interact with their machines, the Internet, various clouds, and the people with whom they communicate. The answer to this question will affect the efficiency of using the Internet and the effectiveness of all Internet users.

As large Internet service providers expand their Internet clouds and remove their software from direct user control, the user faces an increasingly closed Internet. Perhaps the vendors believe they are making their operating systems and browsers more user-friendly. That might be the case, but they are also making their interfaces subject to more cloud influence.

An Iceberg: Net Neutrality or Balkanization?

The opening of the Internet envelope and the increasing intrusion of commercial messages onto user screens sit atop an iceberg. Resting below the surface of the iceberg lie the issues of privacy, security, quality of service, unsolicited advertising, and loss of control.

Other countries are involved in similar debates. What might be the outcome of these deliberations? Should Internet usage be subject to restrictions? Should Internet usage be priced? Using topical jargon, should certain parties be granted fast lanes on the Internet highway? Can others be placed in slow lanes and still receive adequate service to meet their needs? Will commercial clouds take over an Internet user's sessions?



Estimated monthly cost for 25 megabits per second, the speed at which a YouTube video loads in 1.3 seconds and a two-hour movie in 13.3 minutes

If the United States government imposes different rules on Internet usage than, say, the European Union, how will the Internet adjust its vast inventories of hardware and software — which reflect geopolitical leanings and associated cultures — to accommodate different philosophies? Because of political and philosophical differences that exist between countries, these divergences might lead to the balkanization of the Internet into different networks that are tailored to national boundaries. The result will be an awkward set of incompatible systems.

Unintended Consequences

The U.S. government surveillance operations are controversial — depending on one's political persuasions. Apart from politics, U.S. businesses stand to lose billions of dollars in revenue because other countries are passing laws forbidding their citizens' data to be sent across country borders. The Internet may be divided into fiefdoms as countries are forced to balkanize parts of the Internet to safeguard their own country's privacy laws.

In October 2014, the European Court of Justice invalidated the Safe Harbor agreement. This accord allowed U.S. enterprises to move data about Europeans outside European borders. Companies such as Google have been placed in difficult positions. More than 4,000 U.S. firms will be affected negatively by the rescinding of this agreement.

America's allies are now making reference to this nation as a surveillance state, an accusation that is both accurate and hypocritical. Compared to whom? China? North Korea? Iran? Even the EU countries have surveillance programs. The United States is just better at it than others.

In addition, like him or hate him, Edward Snowden's actions forced Uncle Sam to come clean, leading to the cessation of illegal activities. America, like other countries, has "wire-tapped" since Mr. Bell asked his assistant for help. With the USA Freedom Act and court decrees, the U.S. is now doing it within the law.

Who Controls?

The title of this article is "Who Controls the Internet?" Perhaps the answer should be: no one. The Internet should continue to exist as a relatively uncontrolled dispenser of bandwidth and services. I use the phrase "relatively uncontrolled" because human nature leans toward taking control, often at the expense of other humans.

Humans created government many years ago to keep watch on themselves. We Americans do not like others looking over our shoulders, but most of us recognize the eyes of Uncle Sam can protect us from some bad actors. In this regard, the FCC Net neutrality rulings show both wisdom and restraint on the part of our government.

The Internet remains an extraordinary creation. Untold numbers of humans depend on the Internet for their personal and professional happiness and livelihoods.

If this multifaceted community, vendors and users alike will pay more respect for humans' privacy on the Internet; if they will foster the creation of discourse extending beyond 140 characters; if they will acknowledge that the Internet's effectiveness is based on fair treatment for all the passengers who use its highways; if they will support placing the user screen under the stewardship of the user, their actions will go a long way toward keeping this extraordinary creation a wondrous tool.

How we treat the Internet now will determine how the Internet treats us in the future.

Uyless Black is an award-winning author who has written 40 books on a variety of subjects. His latest book is titled "2084 and Beyond," a work on the origins and consequences of human aggression. He resides in Coeur d'Alene.

Opinion

Editorial

The giant is kicking David's butt

Today marks the conclusion of an insightful 10-day series on the Internet, penned by local author Uyless Black exclusively for readers of The Press. The series will become part of a book Uyless is writing, and we'll be sure to let you know when that's available.

In the meantime, the series left you with a lot of takeaways. One that impacts you directly is this: The downside to the upside of shopping Amazon for your retail needs.

Amazon's story is inspiring — particularly if you're a stock holder or employee. Not only is the Seattle-based firm the world's largest retailer, but it's getting even bigger because of Amazon Web Services' cloud business. Don't forget, either, the power of Prime. According to the Seattle Times, Amazon signed up 3 million new members to its $99 per year Prime service in the third week of December alone.

Final 2015 figures aren't available yet, but Amazon's revenue in 2013 was $74.45 billion and $88.99 billion in 2014. Certainly, 2015 will show similar or greater growth.

As Mr. Black's series pointed out, however, Amazon's huge appetite is largely being fed at bricks-and-mortar retailers' table.

Shoppers love the convenience and almost limitless selection Amazon offers up and down the price scale. Toss in free shipping, and Amazon is a competitor you don't want to face. But this isn't simply a merchandising war. Our concern is the long-term effect of Amazon and lesser national online retailers on communities.

Granted, local stores need to hit home runs with customer service and competitive pricing. They have to give shoppers ample reason to buy locally. If customers can buy similar products for less money on Amazon, many will. But saving a few dollars will actually hurt them in the long term.

Local retail businesses generate taxes that Amazon does not: property and sales. Many of those dollars are funneled back into the community in a host of significant ways, including paying for our kids' education, paving streets and hiring police and firefighters. These same local retailers support our nonprofits, sponsor youth sports and recreation teams, attend city council and school board meetings, and generally form part of the essential glue that holds our communities together.

Idahoans are supposed to pay their own sales tax by reporting their online purchases from companies like Amazon but, according to the Idaho State Tax Commission, very few do. A 12-member legislative Tax Working Group met last fall to explore streamlined online sales tax collection options, and there's some hope their recommendations can lead to a more equitable approach this session.

However, two things need to change before competition and community can flourish. One is in federal hands. Until online retailers like Amazon are required to collect sales taxes universally and distribute that money to the appropriate states, states are going to have extremely limited ability to recoup the money.

The other thing that needs to change is your frame of mind. Surveys continue to show broad public opposition to the imposition and collection of sales taxes by companies like Amazon. Until citizens decide that Amazon is winning the retail war on an unfair playing field and depriving states and communities of vitally needed revenue in the process, no significant change can be expected. And the fall of local retail businesses, leaving ugly shells where prosperity once lived, won't be lamented until it's much too late.