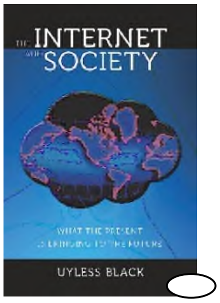


Your on the Street Reporter

Uyless Black

The Internet and You

(Volume I 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.

Opinion

Editorial

Black sheds light on the Internet

Almost everybody uses the Internet, but how many of us have even a basic grasp of this powerful, complex tool?

A local gentleman named Uyless Black does, and lucky for us, he's happy to share much of his Internet research and insights.

In a 10-part series that begins tomorrow, Black will lay out — from an insider's view as well as an adept researcher's — details on key topics. They include:

- Intrusive advertisements
- Net neutrality
- Protecting user content
- Twitter and literacy
- Big data and megadata
- Government surveillance
- Commercial surveillance
- Hard copy and concrete
- Clouds
- Who controls the Internet

Black, who has contributed a handful of intriguing and sometimes controversial articles to The Press over the past couple of years, has written nearly 40 books. The first 35 were on computer networks and the Internet, subjects he also tackled eloquently as an international lecturer.

A U.S. Navy officer during the Vietnam War, Black later was assigned to the U.S. Defense Intelligence Agency, where as a department head he worked with military bases and attaches around the world. From there, Black was assigned to a Navy computer programming facility in the nation's capital, where he wrote software that simulated submarine warfare. That's when he came into contact with administrators from the forerunner to the Internet: ARAPNET.

Black's expertise led him to the Federal Reserve Board, where he wrote the country's first software simulating the nation's money supply. Black worked for the Federal Reserve System for 10 years, going from programmer to assistant director of the Federal Reserve Board. In his spare time, Black earned a master's degree in computer systems at American University and became an adjunct professor to create and teach a new grad course in data communications.

After leaving the Federal Reserve Board, Black went on to own three businesses dealing with computer networks. For 20 years he also consulted with corporate managers and software engineers about data communications network architecture and Internet protocols.

You can read — free, with no advertisements attached — over 200 of Black's essays on Blog.UylessBlack.com. But do that later.

For the next couple of weeks we'll keep your brain busy with Black's 10-part series, exclusively in The Press.

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

Monday
January 4, 2016

Series examines issues for Internet users

Dealing with intrusive advertisements

By UYLESS BLACK
Special to The Press

The Press published a series of articles about the Internet between July 31 and Dec. 15, 2014. They addressed several issues, such as privacy and the U.S. government's plans about the future of the Internet. These subjects will not be revisited in this series. You can find them in the Press archives at cdapress.com.

Black

This article is the first in a series of 10. They are written for an individual Internet user, as well as for companies and other enterprises. Those organizations with an IT department likely have staff members who are familiar with much of this material.

However, even corporate giants have thought they were attuned to Internet issues, only to find themselves out of touch and sometimes in dire straights. They ignored some simple procedures that would have protected their systems against intrusions that compromised their operations.

With these thoughts in mind, we begin this series with a subject that is increasingly drawing the discontent of Internet users: unsolicited advertisements intruding onto user screens. At first glance, this irritating feature might seem to be a relatively minor nuisance. It is that and more, because it also deals with the issue of who controls our Internet sessions.

Postal mail falls, email rises

The use of first class mail in America is declining rapidly. In 2000, the U.S. Postal Service reported it handled 102.4 billion first class pieces. In 2014, that figure had declined to 63.6 billion. In contrast, business email traffic is growing. According to the Radicati Group, a research firm, 100 billion business emails are transmitted every day on the Internet. That figure is predicted to increase to 132 billion by 2017. (Personal email use is declining as non-business consumers move to texting, Twitter, Facebook, and other forms of social media.)

Some futurists predict first class postal mail will become so expensive that its use will become insignificant, confined to a limited population (likely government-subsidized) who do not have access to the Internet. If this situation comes about, online correspondence will become the only viable, inexpensive way to exchange business and personal correspondence.

The questions are: Do we want to live in a world in which we have no control of our user screens? Do we want to be held captive to an ad we cannot remove while we are in need of screen space? Will we continue to tolerate an ad that is placed in front of our own content to the extent we are forced to be idle?

The Internet and you

TODAY: Intrusive advertisements
Tuesday: Net neutrality
Wednesday: Protecting user content
Thursday: Twitter and literacy
Friday: Big data and metadata
Jan. 11: Government surveillance
Jan. 12: Commercial surveillance
Jan. 13: Hard copy and concrete
Jan. 14: All about clouds
Jan. 15: Who controls the Internet

When the Internet was first created, no advertisements were interspersed into an Internet user's traffic. Later, as the computer industry migrated to the use of screens (instead of hard copy), there were still no ads pasted into the user's screen. Initially, the fledging Internet was run by the federal government which did not allow commercial traffic of any kind.

Obviously, times have changed. Advertisements have become so common that some Internet vendors view the system as nothing more than an advertising medium.

Problem is worsening

The lack of users' control over their screens is becoming more pronounced. When I log on to my email account and open a window to key-in text, my part of the screen is frozen until another part of the screen that is reserved for advertisements has been activated, and has sent me unsolicited ads. After a few seconds, the Internet provider frees up my keyboard, and I can enter my mail in a template located on the left side of my screen. During this time, ongoing advertisements are playing on the right side of my screen.

David Pogue, in Scientific American of January 2016, states: "...79 percent of the time it takes for a news Web site to load on your phone is waiting for the ads to arrive." Imagine the lost productivity that comes with this model! I occasionally glance at these intrusions and vow to forego buying any of the peddled merchandise.

How much time do these ads waste while an employee or contractor is putting in paid time at the office? I suspect the figure runs into many millions of dollars.

Ad blockers

One solution is to install an ad blocker. As one example, Apple now supports ad blocking apps for its mobile devices. If you are interested, ask your software or hardware vendor about this package, or surf the Internet for offerings.

The inevitable question arises: How are the Internet vendors going to fund their websites that we visit to get news and other necessities of life, as well as to satisfy our entertainment fixes? The answers to this question are (a) some vendors already derive income by capturing data about users and selling it to others; (b) many Websites are free anyway; (c) the Internet has been commercialized so why not set up a system in which users pay vendors for the "luxury" of having their screens free from advertisements?

Answer (c) is a contradiction to Net neutrality, as this approach is counter to having a classless, egalitarian Internet. One part of Net Neutrality is: Do not allow users with deep pockets to pay their way toward obtaining better service than less affluent customers.

To compound the problem, some sites have installed blockers that block ad blockers. Other vendors will not allow users to access their sites if the users have ad blocking software installed on their machines.

Problem won't just disappear

Many users of the Internet do not understand these arcane issues. Nor should they be asked to know about them. They should have assurances that the soon to be pervasive email, texting, and tweeting services of the Internet will provide the safety, security, privacy, and fairness that has been provided by the devolving U.S. Post Office. The likelihood of online correspondence being given the same privacy and respect as conventional mail is akin to demanding companies such as Google cease doing what allows them to exist in the first place.

Therefore, the growing nuisance of intrusive, unsolicited ads is only the beginning of the Internet losing its neutrality and an associated degradation of the quality of service. It is possible, despite the Net neutrality advocates, that pricing mechanisms will come about that allow users to open up their wallets to keep ads off their screens.

If the Internet evolves in a manner similar to the examples cited in this article, to whom will my Internet service provider give preference during periods of high activity: Uyless Black, a single citizen? Or, say, Apple, a Fortune 500 company? My wallet is not as thick as Apple's.

What is the answer? Is it the strict enforcement of the idea of Net neutrality, where all users are equal and deep pockets cannot buy privileges? Or should the Internet model itself reflect free market doctrines: You get what you pay for?

To address these questions, we examine the issue of Net neutrality. We've skirted around the subject thus far, obtaining enough information to deal with the subjects of intrusive advertisements and screen control. The next article delves into Net neutrality in more detail.

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 5, 2016

The Internet: How Net Neutrality affects you

By UYLESS BLACK
Special to The Press

Black

The Federal Communications Commission has issued rulings to address the subject of Net Neutrality. These decrees are not fully in place, but they are already being challenged by many Internet vendors and factions in Congress.

What is Net Neutrality? FCC explains the term with what it calls "Clear, Bright-Line Rules" to address practices that the agency claims "invariably" harm the Internet:

No Blocking. "Consumers who subscribe to a retail broadband Internet access service must get what they have paid for — access to all (lawful) destinations on the Internet. ...A person engaged in the provision of broadband Internet access service:..shall not block lawful content, applications, services, or non-harmful devices, subject to reasonable network management." [Broadband is a general term to identify companies that own the physical media, such as telephone local loops, TV cable, and wireless channels.)

No Throttling. The throttling of user traffic could

See BLACK, A7

The Internet and you

Monday: Intrusive advertisements
TODAY: Net neutrality.
Wednesday: Protecting user content
Thursday: Twitter and literacy
Friday: Big data and metadata
Jan. 11: Government surveillance
Jan. 12: Commercial surveillance
Jan. 13: Hard copy and concrete
Jan. 14: All about clouds
Jan. 15: Who controls the Internet?

BLACK

from A1

result in the resemblance of traffic blocking. For example, throttling (slowing down) the playback of a movie to the point where the movie has time gaps between the packets containing segments of the movie has the same effect as blocking. In any case, an Internet provider is not allowed to throttle the content of any customer's traffic.

Repeatedly in these rulings, the FCC informs the public it is well aware of the dangers of a multifunction provider possibly throttling content that competes with a content provider's offerings. A multifunction provider is a broadband provider who owns the channels and offers, for example, movies on its broadband channels. Comcast and Time Warner are multifunction providers. Netflix and Facebook are content providers and must rely on Comcast and Time Warner to provide them broadband channels (such as cable, wires, and wireless media).

I am not suggesting that Comcast or Time Warner would exploit their positions of owning the bandwidth that content providers such as Netflix and Facebook need. I am offering that Comcast and Time Warner have part of their operation in the same business as that of Netflix and Google — the same skin in the game.

In one sentence, the commission sums up its thoughts on the subject of Net Neutrality: "America needs more broadband, better broadband, and open broadband networks."

It comes as no surprise that the critics of this statement are the broadband carriers, such as AT&T and Comcast. The content provider companies who rely on the broadband carriers to provide them physical channels are pleased with the FCC rulings. Thus far, Netflix, Spotify, Google and other content providers have won the day. Netflix said, "[The FCC] order is a meaningful step towards ensuring ISPs [broadband channel providers] cannot shift bad conduct upstream to where they interconnect with content providers like Netflix."

The day is far from over. It could be months (even years) before Congress, the White House, and the courts settle the issues. Immediately after the FCC published its rulings in March 2014, the trade group USTelecom, representing many Internet companies such as AT&T and Verizon, filed suit in the US Court of Appeals for the District of Columbia Circuit.

The USTelecom petition claims the FCC ruling violates federal law and is "arbitrary, capricious, and an abuse of discretion." As expected, the battle is on: Media providers vs. content providers. The resolution of the issues will affect all users of the Internet.

Paid Prioritization?

The FCC is particularly concerned about the subject of paid prioritization. The Commission describes it as follows:

Paid prioritization occurs when a broadband provider accepts payment (monetary or otherwise) to manage its network in a way that benefits particular content, applications, services, or devices. To protect against "fast lanes," this Order prohibits the practice of paid prioritization.

The record demonstrates the need for strong action. [A previous court decision has] noted that broadband networks have powerful incentives to accept fees [from various parties], either in return for excluding their competitors or for granting them prioritized access to end users.

Beware of Service Plans

The FCC wishes to implement general rules that apply to all. Therefore, it states a "case-by-case enforcement can be cumbersome." The Commission apparently has come to distrust those service plans you and I try to read just before we fall asleep at our desks. The FCC says, "...where consumer permission is buried in a service plan—the threats of consumer deception and confusion are simply too great."

The last sentence of this FCC quote was included because of consumer complaints about the lengthy contract (service plan) a customer must read and accept before the customer is allowed access to the Internet provider's product. For the average Internet user, these service plans are not much more than robber baron writings. They are so long and so fraught with legal and technical jargon that most users simply give-up and click "I agree" to this contract.

Vendors must protect themselves, and organizations with IT and legal staffs can wade through pages of arcane text that is simply unfathomable to an average Internet user. Yet that very user might consign away control over his/her computer software and not be aware of it.

Be it a cloud, a word processing program, etc., Internet users (companies as well as individuals) must understand scores of these legally-binding terms of agreement. To gain an understanding of the magnitude of the problem, a study was made by Carnegie Mellon University on privacy contracts alone. I was surprised about the findings of the study, as you may be as well:

According to a study by Carnegie Mellon University, the average American encounters 1,462 privacy policies a year, each with an average length of 2,518 words. If one were to read each and every one of these policies, it would take seventy-six full workdays, at eight hours a day, from our lives.

Besides the service contract, the FCC rulings came down on the side of content providers, such as Google, Netflix, and Facebook. The broadband carriers, such as AT&T and Comcast, who provide the physical channels (the bandwidth) for the content providers, claim the FCC's rulings are unfair.

An old adage is brought to mind, "Where one stands depends on where one sits." Who is right, who is wrong on these issues of Net Neutrality? That depends on where one sits.

The FCC quotes in this article are from FCC 15-14, GN Docket No.14-28."

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 6, 2016

The Internet: Protecting user content

By UYLESS BLACK
Special to The Press

It was only a matter of time. The revelations that U.S. government agencies were conducting illegal surveillance on Americans put pressure on Internet vendors to place powerful security protocols in their products. The 2nd U.S. Circuit Court of Appeals in Manhattan said the PATRIOT Act (a set of laws, some of which permit more government surveillance) did not authorize the National Security Agency (NSA) to collect Americans' calling records in bulk.

Black

Consequently, during the past few months, several major companies who provide their customers with access to the Internet, called Internet Service Providers (ISPs), have made advanced cryptographic products available to their customers. The products scramble (encrypt) user data so that it cannot be read by anyone other than those who are able to unscramble (decrypt) the data.

After reading about frequent security breaches at lauded institutions, such as Sony and the United States government, you might be dis-

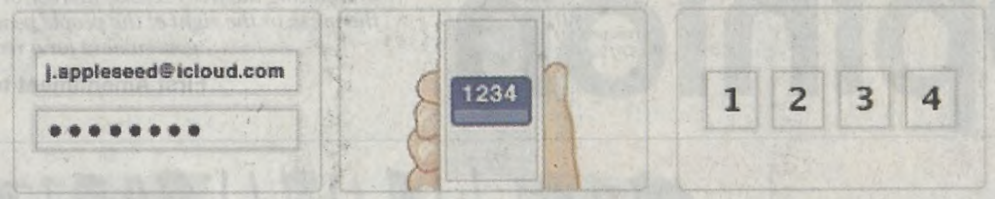
See BLACK, A3

The Internet and you

Monday: Intrusive advertisements
Tuesday: Net neutrality
TODAY: Protecting user content
Thursday: Twitter and literacy
Friday: Big data and metadata
Jan. 11: Government surveillance
Jan. 12: Commercial surveillance
Jan. 13: Hard copy and concrete
Jan. 14: All about clouds
Jan. 15: Who controls the Internet?

BLACK

from A1



You enter your Apple ID and password as usual.

We send a verification code to one of your devices.

You enter the code to verify your identity and complete sign in.

couraged about the seeming futility of obtaining privacy of communications on the Internet. It is evident that user traffic can be intercepted, stored, and analyzed.

For some good news, the user content can rather easily be protected. If a sending user takes a few moments to scramble the data at the sending site and the receiving user unscrambles it at the receiving site, user content is protected. Depending on the product, the operations are almost transparent to a user. In addition, other features of these systems include:

- Verifying that user content has not been altered. As we become more dependent on the Internet, it is probable that assorted hackers, with increasing frequency, will attempt to modify users' traffic. There is a lot of money to be made: Examples are altering a funds transfer, changing the text in a will, or modifying business correspondence.
- Verifying the party that sent the message is the correct party. This feature will also become increasingly important as more business correspondence is carried online. One feature of this attribute is called 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 as being legitimate. 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 for signatures certified by a public notary (depending on local laws).

Be aware that encryption operations must take place in the user machines, and not intermediate nodes along the way, such as routers and servers that belong to third parties. If you allow a third party to become involved in the process, the purpose may be defeated. This concept is called the end-to-end principle. Do not forsake this principle unless you have absolute trust in a third party. As a general rule: Do not trust anyone but yourself and the party with whom you are exchanging traffic.

For the remainder of this article, two security features are highlighted: the Advanced Encryption Standard and the two-step verification procedure. Their descriptions will be of a general nature. The important point is to strongly encourage you to make certain the company that offers security services to you has these technologies in its product line. This recommendation is especially important for organizations (or individuals) who are sending sensitive data over the Internet.

The Advanced Encryption Standard

The Advanced Encryption Standard (AES) is the tool used by Internet vendors and end-users to protect traffic. Thus far, it has proven to be impregnable. It is widely available in most but not all vendor products. If you do not care if your email, text, pictures etc. might be examined by other Internet parties, you may not wish to involve yourself in this process. However, if you or your company must exchange sensitive correspondence — increasingly being done over the Internet — you are running a fool's errand by having your traffic sent in the clear. While AES is not the end-all of crypto systems, it has become a de facto standard in the industry.

Two-Step Verification

One of the most serious security problems facing companies and individuals is hackers discovering their passwords (also referred to as "keys" in some literature). With this information, it is often easy to gain access into a system. To address this problem, an effective security tool is called two-step verification.

It is used to prevent hackers from accessing a user system. This powerful security feature is available from many Internet vendors. I highlight Apple's system, but keep in mind that other companies offer similar capabilities.

What makes two-step authentication effective is that the first part is the password itself, which is something you know. And the second step, according to The Economist, May 30, 2015, user traffic:

"...can be made more robust by being paired with "something you have," which could be a device or app which receives or generates a unique code, known as a token. ... Such gadgets are already widely available in online banking for users to generate a code when accessing their accounts. The code can also be texted to a user's mobile phone when logging into their email on a computer."

Some systems add security questions (such as, what is the maiden name of your mother?) to further enhance the robustness of the system.

To demonstrate how easy it is to use two-step verification, consider Apple's procedures. Apple requires only that a user verify his/her identity by registering one or more of Apple's hardware devices, such as an iPhone.

The figure below is a reproduction of an Apple graphic that illustrates the process. After the completion of these actions, the user later verifies his/her identity by entering both a password and the 4-digit verification code in order to access a site such as iCloud or iTunes. The user is not allowed access unless both the password and verification code are correctly entered. Notice that most of the work is done at Apple's end and not at the user's end.

(SEE ABOVE GRAPHIC)

Nonetheless, you might be asking at this point: "Uyless claims these procedures are simple and easy to use, but they do require effort on my part. Is it worth it?"

I only ask you to read your user's manual or call your security provider, and give it a go. To answer the hypothetical question: What are your family photographs, tax forms, letters — all your Internet files worth to you? Burning a few calories to make your files safe is indeed worth it. I've had clients who have lost files to hackers, a misfortune that drove some of them into depression.

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 7, 2016

The Internet: Tweeting literacy away?

By UYLESS BLACK
Special to The Press

In the latter part of the 20th century, technology became available to allow researchers to examine the detailed structure of the brain. Various techniques, grouped under the name of neuroimaging, can now display the surface and innards of the brain.

The brain has been undergoing changes throughout humans' existence. For this discussion, one neuroimaging project showed that the composition of different areas of the cortex was different for a person versed in playing the violin in contrast to a person who played the piano (See The Brain, A NOVA program series, PBS, fall 2012). One might think that musical talent — string or keyboard — would be confined to one part of the brain, but it is not. Numerous studies show the creation of additional neural connections come about as a result of participating in an ongoing activity for a prolonged time. In effect, the brain rewires itself to accommodate a new pursuit. This transformation takes place to make execution of the activity more efficient.

Black

See BLACK, A5

The Internet and you

Monday: Intrusive advertisements
Tuesday: Net neutrality
Wednesday: Protecting user content
TODAY: Twitter and literacy
Friday: Big data and metadata
Jan. 11: Government surveillance
Jan. 12: Commercial surveillance
Jan. 13: Hard copy and concrete
Jan. 14: All about clouds
Jan. 15: Who controls the Internet?

An example of cerebral rewiring is the use of Twitter. We may have forgotten the time and frustration it took to learn the process. Several hours and many retries were needed to master the ability to key-in text with both thumbs and fingers. As we practiced, we became more proficient.

Our brain can be rewired to optimize new activities, such as playing a musical instrument. It changes its shape as it becomes more adept at coordinating motor and cerebral functions. Why should learning a new task, such as text entry, be any different?

The brain also rewires itself to accommodate the cessation of the practice of an activity. If tasks, once performed on a regular basis, are no longer performed, the brain adjusts accordingly. We forget how to speak a foreign language. We lose the ability to deftly break an eggshell with only a thumb and a palm. We become rusty.

Every human activity has an effect on the brain, and prolonged activity creates a change in its structure and operations. The change may be observable, such as changes that can be seen on the cortexes of piano and violin players who practice extensively on the respective tools of their trade.

What happens to our brains when we stop composing letters or emails? When we stop reading them? What happens when we stop doing what we once did? The brain composition for guiding these executions goes away. Other parts of the brain might take over, rewired to displace what are now nascent activities.

Does that mean that resorting to Twitter instead of email or hard copy dooms a person to illiteracy? Of course not. Nonetheless, it is claimed by some researchers that those who have had little exposure to writing complete sentences, the continuous use of Twitter further degraded their communicative skills.

Not enough text and too much tech?

Images such as those on Facebook and YouTube can be beguiling. However, an automated society — one that increasingly uses software and computer networks to solve problems — runs the risk of thinking of automation as a panacea to society's literacy ills. In so doing, the society risks misusing software at the expense of under-using human labor.

This last statement ight be construed as ating the obvious, it some schools have bstituted the use of imans to teach students id replaced this person- contact and guidance ith computers. As well, irents often forsake eir roles as overseers their children's study id homework.

A study at Duke niversity tracked the arning progress of most one million students in relation to the ates they were given ccess to computers and ie Internet. The study howed that students aving access to Internet-connected computers with little supervision about their use suffered a decline in reading and math scores. Other studies show that unless children are supervised closely by a parent or a teacher, they spend increasingly more time tweeting their friends and playing games rather than using the academic software of the networked computer.

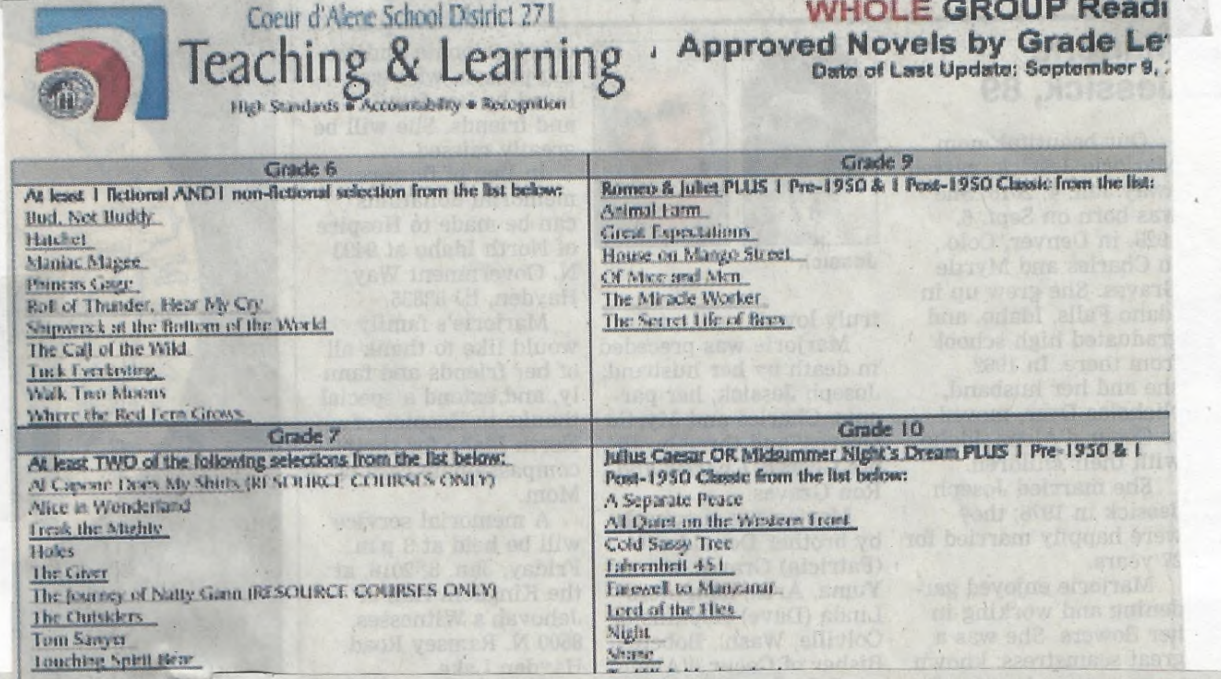
Susan Pinker (in the NOVA program cited earlier) puts it well: "It's drive-by education — adults distribute the laptops and then walk away."

In applying computers and the Internet to education, or for that matter, any endeavor, it is prudent to be aware of the Law of the Instrument, exemplified by the child who picks up a hammer and looks for something to pound. Twitter should not be used to pound everything pertaining to the written word, nor should parents allow their children to engage in such pounding.

Coeur d'Alene Schools:

A model for emulation

I contacted representatives of the local school district where I live in northern Idaho. The information on the Coeur d'Alene School District 271 website and the correspondence I exchanged with the representatives of this district gave this writer encouragement that "tweeting away literacy" is being held at bay by some far-sighted educational institutions. Mike Nelson, the Director of Curriculum and Assessments wrote me:



Coeur d'Alene School District 271

Teaching & Learning

High Standards • Accountability • Recognition

WHOLE GROUP Readi

Approved Novels by Grade Le

Date of Last Update: September 9,

Grade 6	Grade 9
At least 1 fictional AND 1 non-fictional selection from the list below: Bud, Not Buddy Hatchet Maniac Magee Phineas Gage Roll of Thunder, Hear My Cry Shipwreck at the Bottom of the World The Call of the Wild Tuck Everlasting Walk Two Moons Where the Red Fern Grows	Romeo & Juliet PLUS 1 Pre-1950 & 1 Post-1950 Classic from the list: Animal Farm Great Expectations House on Mango Street Of Mice and Men The Miracle Worker The Secret Life of Bees
Grade 7	**Grade 10**
At least TWO of the following selections from the list below: Al Capone Does My Shirts (RESOURCE COURSES ONLY) Alice in Wonderland Freak the Mighty Holes The Giver The Journey of Natty Gann (RESOURCE COURSES ONLY) The Outsiders Tom Sawyer Touching Spirit Bear	Julius Caesar OR Midsummer Night's Dream PLUS 1 Pre-1950 & 1 Post-1950 Classic from the list below: A Separate Peace All Quiet on the Western Front Cold Sassy Tree Fahrenheit 451 Farewell to Manzanar Lord of the Flies Night Shane

"You would be surprised but we still do a great deal of sentence diagramming. Our curriculum has spiraled instruction that includes grammar and syntax in each grade level with the inclusion of literature starting in grades 04 and 05. In each year, we reinforce good grammar through fiction and non-fiction literature ending with British literature in grade 12. ...Yes, even though society may communicate in 140 characters outside of our school walls, our district insists on writing with conviction and purpose..."

Sentence diagramming was a curse during my teenage years. I hated its rigor. I found distasteful its insistence on speaking and writing with a semblance of structure. Yet, in spite of my teenage sloth, this part of my education forced me to come to grips with the architecture of the English language. Even against my conscious will, it subconsciously inculcated into me a smattering of understanding about the composition of my language.

Laura Rumpler, also of Coeur d'Alene School District 271, directed me to a webpage containing lists of books the school requires its students to read. The figure below shows a partial list of books (for grades 6, 7, 9, and 10).

As I read this list, I was encouraged, but I was also reminded of articles I have read about the reading curriculum of many inner city schools. Some of the high school students read at the grade school level. Having gone through college, Dexter Manley, the affable all-pro Washington Redskins football player, informed a Senate subcommittee he was essentially illiterate.

The Twitters of this world are not to blame for this astounding situation, nor is the Internet. Indeed, some anecdotal studies claim youngsters in poor African countries have improved their reading and writing skills by using texting applications.

(SEE ABOVE GRAPHIC)

As a parent, granted of a now quite mature adult, I hope each mother and father reading this article will take it upon themselves to follow the lead of the Coeur d'Alene schools and insist on their children doing more with our subtle, elegant language than abbreviated texting.

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 8, 2016

The Internet: The power of 'bigmeta'

By UYLESS BLACK
Special to The Press

How is it possible that marketing firms and intelligence agencies seem to know so much about us? Advertisements appear on our screens about products we actually like. Intelligence agents know where we are going before we arrive at our destination. Part of this powerful intuition is based on a technology known collectively as Big Data and metadata.

Black

During the past few years, the terms Big Data and metadata have found their way into Internet lexicon. (I do not know why the words Big Data begin in caps.) A more accurate term is Much Data, but Big Data is used in this article because it is the popular saying.

Big Data and metadata processing take advantage of large sets of data to detect trends, identify tendencies, and find relationships in a very large set of data. In many situations, the amount of data is so huge it does not lend itself to conventional analysis, one in which a limited data set size (the amount of data) might be examined by a

See BLACK, A7

The Internet and you

Monday: Intrusive advertisements
Tuesday: Net neutrality
Wednesday: Protecting user content
Thursday: Twitter and literacy
TODAY: Big data and metadata
Jan. 11: Government surveillance
Jan. 12: Commercial surveillance
Jan. 13: Hard copy and concrete
Jan. 14: All about clouds
Jan. 15: Who controls the Internet?

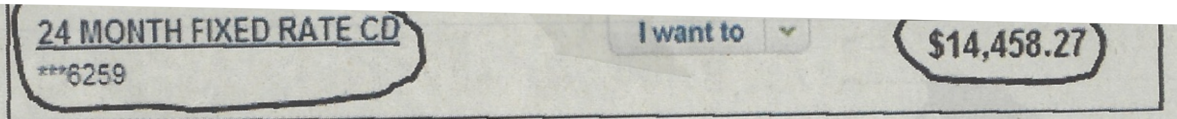

24 MONTH FIXED RATE CD
***6259
$14,458.27

Figure 10-1. Metadata and user content.

BLACK

from A1

single computer to extrapolate information.

Big Data considers a few million characters of data a paltry amount. As one example, the NSA Utah Data Center is reported to be capable of storing exabytes of data, expressed as 1,000,000,000,000,000,000 bytes, a number almost beyond comprehension (in this example, a byte represents a character or a numeral). Clearly, this amount of data cannot be manipulated, much less analyzed with conventional computer processing methods.

For metadata, the most common definition is: "data about data." To clarify this term, see the figure included with this article. The information circled on the left side of the figure is metadata. The information circled on the right side of the figure is data: user content.

See Figure 10-1, Metadata and user content, above

The information of "24 MONTH FIXED RATE CD ***6259" is data about data. It identifies account number 6259, which is a 24-month fixed rate certificate of deposit. The data itself, user content, is the value of the CD: "$14,458.27."

Metadata can contain considerable information about the owner of the metadata. In this example, if metadata were made available to parties such as Internet vendors (Google, for example), government agencies (NSA, as an example), a certificates of deposit thief, a terrorist group, a former spouse, etc., the owner of the metadata is vulnerable to having his/her private transaction with a bank disclosed.

Of course, this one metadata record reveals only tidbits about the owner of this CD. However, if a snooper can capture all the banking records of this party, the snooper can manipulate and infer a considerable amount of intelligence from this so-called non-personal data. This example is restricted to bank deposits. Yet metadata exists for practically any subject, such as medical information, sexual interests, shopping habits, marital accords and discords, etc.

Bigmeta

To process billions of pieces of data and metadata, enormous computer resources are required. Some organizations have thousands of computers networked together to analyze both data and metadata. I have coined a new term to identify the use of huge computer resources to massage both data and metadata: bigmeta. Granted, it is a contrived word, but succinctly identifies two technologies and associated computer power.

How does Bigmeta work?

The relationships of the data elements in bigmeta files are important. For example, if during the examination of a massive set of data, a suspected drug dealer is discovered to be calling a number often, this phone number will be examined further. At a minimum, the analysis will determine the identity of the called party, and correlate this party to other calls this party receives and sends. Some bigmeta systems then predict the likelihood of traits that might be associated with the people using these data elements.

According to bigmeta experts, with other information (movements, location, habits, etc.), accurate assessments can be made about these people being (or not being) in the drug trade. I emphasize "with other information," because bigmeta is often able to show relationships between seemingly unrelated events.

Hammering data yields extraordinary results

Some parties call this approach hammering the data. The slang term conveys the idea that with enough data and with enough computer processing power, information can be gleaned from what might appear to be irrelevant data relationships. This hammering has shown to have results. Alex Pentland, an MIT scientist, is the author of a new book on a subject he calls "social physics."

"The power of [bigmeta]," he says, "is that it is information about people's behavior instead of information about their beliefs. It's about the behavior of customers, employees, and prospects for your new business. It's not about the things you post on Facebook, and it's not about your searches on Google, which is what most people think about, and it's not data from internal company processes. …This sort of [bigmeta] comes from things like location data [from] your cell phone or credit card; it's the little data breadcrumbs that you leave behind you as you move around in the world."

"What those breadcrumbs tell," he continues, "is the story of your life. It tells what you've chosen to do. That's very different from what you put on Facebook. What you put on Facebook is what you would like to tell people, edited according to the standards of the day. Who you actually are is determined by where you spend time, and which things you buy. [Bigmeta] is increasingly about real behavior, and by analyzing this sort of data, scientists can tell an enormous amount about you. They can tell whether you are the sort of person who will pay back loans. They can tell you if you're likely to get diabetes."

Metadata alone: A powerful solo actor

David Cole wrote an article on the power of metadata (See http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/.) Cole's article states:

But metadata alone can provide an extremely detailed picture of a person's most intimate associations and interests, and it's actually much easier as a technological matter to search huge amounts of metadata [the Bigmeta approach] than to listen to millions of phone calls. As NSA General Counsel Stewart Baker has said, "Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." When I quoted Baker at a recent debate at Johns Hopkins University, my opponent, General Michael Hayden, former director of the NSA and the CIA, called Baker's comment "absolutely correct," and raised him one, asserting, "We kill people based on metadata."

Big Data, metadata, and thousands of cooperating computers yield bigmeta. Their inferential power is astounding. They protect ordinary citizens from potential harm from terrorists. They give terrorists information about their intended targets. They protect enterprises from hackers. They give hackers additional tools to penetrate enterprises.

For you, me, and groups of organizations, our data and metadata are fodder for the digital farms belonging to Internet vendors and surveillance agencies. We are the silage that feed their bigmeta organisms.

Does this aspect of our online world bother you? Is it your concern that in the future, Orwell's 1984 could come to pass in 2084? It's once again reflective of the old saying: "Where you stand is where you sit."

The Internet advertisers and surveillance organizations are happy as larks about bigmeta technology. How it will evolve to be used will be a key part of how our societies cope with protecting our safety and at the same time, protecting our privacy.

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