PRIVACY AND SECURITY ON THE WEB –

HAVE MARKETERS AND THE FEDERAL GOVERNMENT GONE TOO FAR?

MICHAEL LATTA, WALL COLLEGE, COASTAL CAROLINA UNIVERSITY

ABSTRACT

Privacy and security on the web has emerged as a major government policy and marketing issue. Everyone from politicians to children will be affected by regulation of the internet and the construction of gigantic data warehouses. The recent breaches in security and privacy by hackers and agencies of the Federal Government, and the common practice of planting software on home computers to track users online have negatively affected public perceptions of surveillance on the internet. Younger users may not be as aware of the extent and intrusive nature of tracking and surveillance as are older adults. This differential reaction may be due to the spread of social media. Recently, the Federal Government has been building vast data warehouses to store information about citizens and their daily activities. Regulation of marketing practices is probably inevitable even if the regulations are obsolete as soon as they are written. But, who will regulate the Federal agencies and their use of personal information concerning citizens. This study is an attempt to determine how concerned the public is about advertisers, companies, and the Federal Government collecting information about them. Issues are raised in several aspects of the modern internet and electronic communications era before the giant Federal data warehouses are built by the end of 2013.

THI NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

"The National Security Agency/Central Security Service (NSA/CSS) is home to America's codemakers and codebreakers." This description is now attached to the Federal agency created in 1972 to provide services and products to the Department of Defense, Central Intelligence Agency, and other security related entities both public and private. More recently, the NSA created the Domestic Surveillance Directorate. The Directorate was created after October 2008, when the Federal Government infused $125 billion into nine of the largest US banks to avert a banking crisis. Another $125 billion was also sent to smaller banks to keep them afloat. These infusions of capital were part of the government rescue of the financial system. This activity gave Federal access to each bank's credit card processing system thereby integrating each bank with the NSA's 470,000-square-foot data mining facility in San Antonio, Texas.

As noted on the NSA's website, "The new Citizen Data Warehouse System (CDWS) will create a comprehensive database containing detailed information about each U.S. citizen. Since the vast majority of all U.S. credit card transactions will be fed through this new system, the depth of information will be

unparalleled. Intelligent routing of this citizen data throughout the inter-connected computer systems of various federal agencies will provide citizens a new level of service from the federal government."

Exactly what service is to be provided remains to be seen but may include the description below:

- The description of the facilities involved continues with the following: "Let's say you purchase an airline ticket for an international destination using a credit card. A copy of this transaction will be forwarded to the new NSA data mining facility in San Antonio and then transmitted to various federal agencies. If there are any travel advisories for your destination, you will be automatically notified by the State Department. Should some sort of natural disaster strike while you are on your trip, the local US embassy will already have your contact information. If there are any health concerns regarding your destination, the Center for Disease Control will email you in advance regarding recommended vaccinations. Plus, the FAA will contact you on the day of your trip if there are any expected air traffic delays. The information-sharing possibilities are endless.

Personally identifiable credit card transaction data for:

- Groceries and medications will be routed to the Food and Drug Administration
- Alcohol and cigarette purchases will be routed to the National Institutes of Health
- Battery, light bulb, and gasoline purchases will be routed to the Department of Energy
- Children's books and video purchases will be routed to the Department of Education
- Children's toys and appliances to the Consumer Product Safety Commission
- Cell phone, radio, and walkie talkie purchases will be routed to the FCC
- Hunting rifles and fishing rods will be routed to the Department of the Interior
- And everything else will be routed to the Department of Justice for safekeeping

In an effort to provide even better government services, the NSA has developed special software that unobtrusively collects important information about American consumers in their homes and offices."

The description of data collection continues with a software and hardware list:

"While we prefer not to use the term "Flame virus", this data collection program is designed to remotely control common computer functions such as logging keyboard strokes, activating computer microphones and cameras, taking computer screen shots, extracting geolocation data from images, downloading personal files, and sending and receiving commands and data through Bluetooth wireless technology. To reduce the impact on our citizens, the remote data collection program can be periodically embedded in routine operating system software updates. This information will be transmitted for processing and storage in our new $2 billion NSA data center in Bluffdale, Utah scheduled to open in September 2013."

However, transparency is apparently not complete:

"For security reasons, it is unrealistic to expect a complete list of information we collect for our national citizen database. In the spirit of openness and transparency however, here is a partial list:

- internet searches
- websites visited
- emails sent and received
- social media activity (Facebook, Twitter, etc)
- blogging activity including posts read, written, and commented on
- videos watched and/or uploaded online
- photos viewed and/or uploaded online
- music downloads

- mobile phone GPS-location data
- mobile phone apps downloaded
- phone call records
- text messages sent and received
- online purchases and auction transactions
- bookstore receipts
- credit card/ debit card transactions
- bank statements
- cable television shows watched and recorded
- commuter toll records
- parking receipts
- electronic bus and subway passes / Smartpasses
- travel itineraries
- border crossings
- surveillance cameras
- medical information including diagnoses and treatments
- prescription drug purchases
- guns and ammunition sales
- educational records
- arrest records
- driver license information"

Further description of the data collection techniques includes:

"NSA technicians have installed intercept stations at key junction points, or switches, throughout the country. These switches are located in large windowless buildings owned by the major telecommunication companies and control the domestic internet traffic flow across the nation. A fiber optic splitter is placed on the incoming communication lines and routes the traffic to an NSA intercept station for processing. Eventually, all of the domestic data flow will be routed to the new Utah Data Center when it opens in Fall 2013. The NSA also monitors all satellite communications in and out of the U.S. via satellite receivers located across the country.

In addition to NSA data collection activities, the Domestic Surveillance Directorate receives a constant flow of information from other sources. Some sources are secret and some are public. Public sources include:

- FBI - Information collected from the use of National Security Letters authorized by the PATRIOT Act; Phone calls and text messages from the FBI Digital Collection System (DCSNet); "Google-like" search capability of citizen information from the FBI Law Enforcement National Data Exchange Program; Cell phone location tracking from the Stingray "IMSI catchers" (International Mobile Subscriber Identity) masquerading as cell phone towers.
- CIA - The Central Intelligence Agency has publicly committed to increasing its data collection efforts. CIA Chief Technology Officer Gus Hunt explains why: "The value of any piece of information is only known when you can connect it with something else that arrives at a future point in time. Since you can't connect dots you don't have, we fundamentally try to collect everything and hang on to it forever.
- DHS - TSA airline passenger data; surveillance data from unmanned domestic Predator B drones patrolling the northern and southern borders.
- Treasury - Cash Transaction Reporting and Suspicious Activity Reporting data .

- State/Local government - Electronic transit cards transactions; electronic toll collectors; vehicle information and location data captured by license plate readers; public transportation video/audio surveillance systems."

With data warehouses in San Antonio, Texas, Oak Ridge, Tennessee, and at Camp Williams near Bluffdale, Utah and Fusion Centers throughout the country allows continuous surveillance of citizens with indefinite storage of data concerning every aspect of their lives.

Background to Marketing Security and Privacy Concerns

The internet defines the intersection of public policy and marketing activities in a new and complicated way. While a great deal of effort has been put into discussion of 'Net Neutrality' [4] [5], that policy issue is more of a concern to broadband providers like Comcast and Verizon than it is to the public. Privacy and security in purchasing products (Amazon) or membership on social media sites (Facebook) on the web create policy issues more relevant to the public [6] [12]. On the self-regulation front, The American Marketing Association Code of Ethics for Marketing on the Internet covers privacy, ownership of information, and access to information. However, this code is being ignored by many businesses on the internet using tracking technology. This situation has been worsened by the advent of social media websites where information is routinely shared [3] and by data mining where huge caches of data are exploited for marketing purposes[10].

When Google first sent out its 'bots' to comb the internet, the seeds of internet security and privacy concerns were sown [2]. Google's website says it collects data from users, not including names or other personal identifiers. Names, credit card information, phone numbers, credit history, and purchases are collected from those who opt-in to use Google Checkout to make online purchases. Some marketing companies create pop up ads offering such things as free phone cards to get web users to allow them to track their web activities and preferences.

Marketing researchers are drowning in data from customer activities in web surfing and use of online purchasing, social media, and gaming portals. Some software companies like SPSS have partnered with IBM to create data mining programs that utilize such tracking data for marketing purposes [10]. In the process, a company name like Google, has become a verb; to Google or Google it.

Technology has evolved to the extent that privacy and security policy and marketing issues revolve around what is known as behavioral tracking [8]. Behavioral tracking means following an individual web surfer over multiple websites and over time using several technologies including:

1. Traditional HTML Cookies may be placed on any computer by a website or a script running ads. These Cookies are easily detected and erased by the user or antivirus software.
2. Flash Cookies stored outside the browser can 'resurrect' HTML Cookies that have been deleted. Flash Cookies are more difficult for a user to detect and erase. These Cookies are sometimes called Ever Cookies for that reason.
3. DPI or Deep Packet Inspection of unencrypted information that may flow from one server to another as occurs on any Internet Service Provider (ISP) network when a game system like a Wii is installed and used on a TV.
4. Tracking Software deliberately placed on a computer to record web browsing history, key strokes, or other data.

Extent of Tracking and Data Utilization by Marketers

The Wall Street Journal has claimed that business web sites for large U.S. corporations are extraordinarily intrusive and may employ more than 100 different tracking tools to gather data on customers who visit a website. Some of them use the data only in-house [1]. There are tracking specialist businesses that have created a new business model who collect customer data and sell data and predictions about what customers will do in the future using their past activities and interests. This use of tracking data is called Predictive Analytics and can be done in 'real time.' This research approach is so technical and powerful it has spawned a highly specialized MBA program at Northwestern University and makes customer online tracking the leading edge of marketing research activity.

Research on the Issues

In an industry sponsored assessment of voluntary disclosures of consumer information policies on company websites, [6] it was found that 67% of 361 websites posted a privacy policy, but only 15% were comprehensive in nature and conforming to the AMA guidelines. The policy question is whether or not marketing trade-group rules for self-regulation are good enough to protect consumers, or are regulations and laws needed? In a consumer perceptions study, [12] it was found that consumers consider security concerns (49.8%) more important that privacy concerns (16.0%) in online shopping. To date, the Federal Trade Commission has not recommended legislation be passed governing internet security and privacy.

Privacy, Security, and Tracking Concerns

In a carefully conducted study of the various web tracking technologies, the Wall Street Journal delved into the issues of privacy and security. In a broad based survey of 14,632 internet users done by the Wall Street Journal, the question was asked: 'How concerned are you about advertisers and companies tracking your behavior across the Web?' [14]. The results indicated that 60% of the participants were very concerned about tracking. A Spring 2011 survey of 19 faculty in the Wall College of Business Administration at Coastal Carolina University indicated only 21% were very concerned about tracking.

The unregulated nature of this online activity will probably not last a long time unless a professional organization like the American Marketing Association can supply specific guidelines and lobby to keep the internet relatively free for marketing. The advocates for legislation and regulation may be able to use privacy and security concerns among the public to take over the internet and shut off a rich data source from internet traffic and social media. As the Wall Street Journal study authors ask: 'Are we giving away too much personal data about ourselves, that is then sold to advertisers in exchange for the convenience of having sites remember our passwords? What is lost and what is gained by the technology?'

Sites Feed Personal Details to New Tracking Industry for Marketing Purposes

Recently the Wall Street Journal also published a major study on internet privacy [1]. Large company websites are tracking individuals visiting company sites. These data-gatherers are establishing a new business model using cookies, bots, and beacons to gather and sell raw data about consumers in real time. The companies that routinely use tracking tools are Google Inc., Microsoft, and Quantcast Corp., all of which are in the business of targeting ads at people online.

Google, Microsoft, and Quantcast all say as a matter of policy they do not track individuals by name and offer Internet users a way to opt-out of their tracking networks. However, the state of the tracking art is growing increasingly intrusive, with real time recording of keystrokes and then transmitting them to a data-gathering company that analyzes it for content, tone, and clues to a person's social media site memberships. Other technology can reactivate cookies and other tools that were deleted by the user.

Protective software like Trend Microsystems, Symantec, and Windows defenses are unable to prevent installation and reactivation many times.

Tracking companies and their customers in the ad industry say tracking does not violate anyone's privacy or security because the data sold does not identify people by name, and the tracking activity is disclosed in privacy policies. That may be the case, but consumers still have security and privacy concerns [6].

Students Do Not See the Problem

The most avid users of the web are students. Public policy and marketing impact them more than other age groups in the area of internet privacy. In a survey of University of Minnesota Students[13], some interesting findings were: 33% of students believed that "their Internet activities are anonymous,85% have visited a social networking website,73% are a member of at least one site with 63% members of Facebook, 32% members of MySpace, and 27% members of both, just over half "trust online companies and organizations to keep information about them private," nearly one quarter "say they feel safe making purchases online," but 80% "are concerned that someone could steal their identity using personal information found on the Internet."

A survey of 56 Wall College of Business Administration students at Coastal Carolina University showed these students believe ethical scandals differentiate ethical from non-ethical businesses (75%), they worsen perceptions of business (50%), and that they have no direct impact on perceptions of business schools (57%). Regardless of these results, students will not reduce their use of the internet or social media as a result.

A NEW SURVEY OF CONCERNS ABOUT BUSINESS AND GOVERNMENT SURVEILLANCE OF INDIVIDUAL CITIZENS: METHODS

A sample of 48 students and 32 Faculty/Staff at a small liberal arts University was asked to respond to questions concerning their level of concern with surveillance of individual citizens by advertisers, businesses, and Federal Government Agencies. The response scale used was identical to the Wall Street Journal survey and included the following response categories:

- Very Concerned
- Somewhat Concerned
- Neutral
- Not a Big Worry
- Could Not Care Less

The marketing question included the stem:

How concerned are you about advertisers and companies tracking your behavior across the Web?
The Federal Agency questions were taken from the Domestic Surveillance Directorate's list of 28 data types collected and stored.

The questionnaire is in the Appendix. As a check on consistency the first and last item for the Federal Agency list was identical and related to internet searches since most people have done an internet search even if they are technologically challenged.

RESULTS

The percentage responding "Very Concerned" to the questionnaire items for the total sample, students, and faculty/staff groupings appear in Table 1 below.

Table 1
Percentage Very Concerned About Tracking by Advertisers, Companies and the Federal Government Domestic Surveillance

Tracking	Total % Very Concerned	Student % Very Concerned	Faculty/Staff % Very Concerned
Federal tracking of bank statements	53	48	59
Federal tracking of text messages sent and received	47	43	53
Federal tracking of emails sent and received*	46	40	56
Federal tracking of mobile phone GPS-location data	46	40	56
Federal tracking of credit card/ debit card transactions	45	39	53
Federal tracking of phone call records	41	35	50
Federal tracking of medical information including diagnoses and treatments***	37	28	50
Federal tracking of guns and ammunition sales	33	32	34
Federal tracking of prescription drug purchases***	29	21	41
Federal tracking of internet searches 1**	28	23	34

Federal tracking of surveillance cameras	28	24	34
Federal tracking of internet searches 2**	28	23	34
Federal tracking of online purchases and auction transactions*	27	21	34
Federal tracking of websites visited	26	23	31
Tracking by Advertisers and Companies	**24**	**19**	**31**
Federal tracking of social media activity (Facebook, Twitter, etc)	24	21	28
Federal tracking of photos viewed and/or uploaded online	24	21	29
Federal tracking of videos watched and/or uploaded online	23	19	28
Federal tracking of mobile phone apps downloaded	21	17	28
Federal tracking of blogging activity including posts read, written, and commented on - View our patent	20	19	22
Federal tracking of cable television shows watched and recorded	19	13	28
Federal tracking of travel itineraries	19	17	23
Federal tracking of border crossings	18	15	22
Federal tracking of arrest records	18	15	22

Federal tracking of driver license information	18	15	22
Federal tracking of bookstore receipts**	17	11	26
Federal tracking of commuter toll records	17	15	19
Federal tracking of educational records*	17	13	22
Federal tracking of music downloads	15	13	19
Federal tracking of electronic bus and subway passes / Smartpasses*	15	15	16
Federal tracking of parking receipts*	14	13	16

Chi Square significant at $p < .10$ *, $p<.05$**, $p<.01$***

Responses to the first and last item were identical and showed consistency across the sample. Fourteen instances of Federal Agency tracking elicited a higher percentage of 'Very Concerned' citizens than those who were 'Very Concerned' about advertisers and companies. Most of these items concern personal financial information, communication channels, and medical records; but also included guns and ammunition and general surveillance activities of the Federal Government.

DISCUSSION

Online shopping and banking as well as social media memberships and coupon aggregators like Groupon all provide convenience and a way to find exactly what the consumer wants. Even though security and privacy risks are substantial, students are still heavy users of the internet. The next wave of technology, Near Field Communication (NFC), will soon be implemented by Google Wallet with Master Card, Inc., First Data Corp., and Citigroup, Inc., plus a variety of retailers like American Eagle Outfitters, Walgreen Co., Macy's, and Subway to allow smart phones to make payments with a wave of the card from credit accounts stored on the phone itself. The security and privacy settings on those smart phones will be of high importance in an opt-in system like Google Wallet. Like ATM cards, the 'digital wallet' may turn out to be a risky payment option. All of these extensions of technology that put the public at risk for security and privacy breeches will most likely draw the attention of the Federal Trade Commission and Congress. But the advantages of the digital marketplace have so far out-weighed the risks in the mind of the consumer.

Co-founders Larry Page and Sergey Brin brought Google to life in September 1998. From the beginning, Google's mission was to organize the world's information and make it universally accessible and useful.

The Google service package is 'free,' paid for by advertising dollars of those who seek to market to Google's users [9]. Mark Zuckerberg launched Facebook in 2004 and bought the domain name facebook.com in 2005 to provide an online meeting house known as a social network. Google, Facebook, and other web companies are more about marketing than anything else including risk, security, public policy, and legislation. As a true innovation much like the iPhone, Google has changed the way we live. This change occurred by bringing to the user only relevant information to solve a problem. Are you trying to find someone, something, or someplace? Google it! Regulation and legislation could kill the revolution Google started, but may be inevitable.

On the Federal Agency side, the recent IRS scandals involving targeting political opponents and members of the press have raised concerns about an intrusive Federal Government. The Utah Data Center, which is only one of three giant Federal data centers, was designed to be capable of storing data on the scale of yottabytes (1 yottabyte = 1 trillion terabytes, or 1 quadrillion gigabytes). Its public purpose is to assist in the operations of the Comprehensive National Cybersecurity Initiative (CNCI), though its precise mission of course is secret. A popular TV series, 'Person of Interest,' has the storyline of a massive Federal surveillance system having the ability to identify a single individual and track them at any time to any place. The constitutional and policy implications of the existence of the Domestic Surveillance Directorate's list of 28 data types collected and stored, presumably forever, are just now entering the public's consciousness. Will this Federal surveillance system also change the way we live as Google did? Only further research will tell the tale.

REFERENCES

[1] Angwin, J. and McGinty, T. (2011), "Sites Feed Personal Details to New Tracking Industry," [On-line]. Available: http://online.wsj.com/article/SB10001424052748704584804575645074178700984.html. Accessed: 05/18/11.

[2] Auletta, Ken (2010), *Googled – The End of the World as We Know It (pp, 189-190),* New York, NY: Penguin Books.

[3] Boorman, Chris (2011), "Why Data Mining Is the Next Frontier for Social Media Marketing," [On-line]. Available: http://mashable.com/2011/02/25/data-mining-social-marketing/. Accessed: 05/18/11.

[4] Choi, Jay Pil (2010), "Net Neutrality and Investment Incentives," *RAND Journal of Economics*, 41(3):446-471.

[5] Crowcroft, Jon (2007), "Net Neutrality: The Technical Side of the Debate: A White Paper, *ACM SIGCOMM Computer Communication Review*, 37(1): 49-55.

[6] Culnan, Mary J.(2000), "Protecting Privacy Online: Is Self-Regulation Working?," *Journal of Public Policy & Marketing*, 19(1): 20-26.

[7] Domestic Surveillance Directorate, http://whitehouse.gov1.info/nsa/. Accessed: 05/18/13.

[8] Glazer, Patrick (2011), "How Are Companies Using Online Behavioral Tracking for Research?", *Alert!Magazine*, 51(6): 42.

[9] Goldman, Aaron (2011), *Everything I Know about Marketing I Learned from Google (pp. 1-11),* New York, NY: McGraw-Hill Companies, Inc.

[10] IBM Document Number IMW14282USEN,(2011), "SPSS: Modeling: Three Proven Methods to Achieve a Higher ROI from Data Mining," [On-line]. Available: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=IMW14282USEN. Accessed: 05/18/11.

[11] Marketing Workshop, Inc., (2005), "Ethics and the Company You Keep" survey for the American Marketing Association.

[12] Miyazaki, Anthony D., and Fernandez, A. , (2001), "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *The Journal of Consumer Affairs*, 35(1): 27-44.

[13] Research, Social Networking Services, (2007), "Minnesota Survey of College Students' Internet Use and Privacy Attitudes," [On-line]. Available: http://mistakengoal.com/blog/2007/01/19/minnesota-survey-of-college-students-internet-use-and-privacy-attitudes/. Accessed 07/07/11.

[14] Wall Street Journal Community (2011), "How concerned are you about advertisers and companies tracking your behavior across the Web?," [On-line]. Available: http://online.wsj.com/community/groups/media-marketing-267/topics/how-concerned-you-about-advertisers. Accessed: 05/18/11.

APPENDIX

A study of how people view issues related to business ethics and privacy, is being conducted. If you volunteer to participate, it will take about 3 minutes of your time. There is no consequence to not participating. Also, none of your individual answers will be shared with other people, and your name will not be connected with your answers in any way. The information gathered will be reported in group summary form and will be used to describe people in general. If you would like to participate, please begin by answering the questions below.

PLEASE RETURN THIS SURVEY TO CAROL

For each item below, please **check only one option**.

1. Who are you? _____Undergraduate Student _____MBA Student _____Faculty _____Staff _____Administration
2. Are you: _____ Male OR _____ Female
3. How concerned are you about **advertisers and companies** tracking your behavior across the Web?

Check only one of the 4 options below.

Very concerned	
Somewhat concerned	
Neutral	
Not a Big Worry	
Could Not Care Less	

4. How concerned are you about **Federal Government Agencies** such as the Domestic Surveillance Directorate and Home Land Security collecting data about you from the following sources?

Check only one of the 4 options for each source below.

Source	Very Concerned	Somewhat Concerned	Neutral	Not a Big Worry	Could Not Care Less

internet searches					
websites visited					
emails sent and received					
social media activity (Facebook, Twitter, etc)					
blogging activity including posts read, written, and commented on - View our patent					
videos watched and/or uploaded online					
photos viewed and/or uploaded online					
music downloads					
mobile phone GPS-location data					
mobile phone apps downloaded					
phone call records					
text messages sent and received					
online purchases and auction transactions					
bookstore receipts					
credit card/ debit card transactions					
bank statements					
cable television shows watched and recorded					
commuter toll records					
parking receipts					
electronic bus and subway passes / Smartpasses					
travel itineraries					
border crossings					
surveillance cameras					
medical information including diagnoses and treatments					
prescription drug purchases					
guns and ammunition sales					
educational records					
arrest records					
driver license information					
internet searches					

Thank You For Your Help **PLEASE RETURN THIS SURVEY TO CAROL**