Communications of the IIMA

Volume 12 | Issue 2 Article 2

2012

The Ethics of BI with Private and Public Entities

Brian Demilia
Quinnipiac University

Michael Peded
Quinnipiac University

Kenneth Jorgensen
Quinnipiac University

Ramesh Subramanian
Quinnipiac University

The Ethics of BI with Private and Public Entities

Brian Demilia
Michael Peded
Kenneth Jorgensen
Ramesh Subramanian
Ramesh.Subramanian@quinnipiac.edu
Quinnipiac University
Hamden, CT 06518

ABSTRACT

The Internet plays a vital role in data collection, information creation, and business intelligence (BI). The nature of information collected on the Internet, and the degree to which such information is collected, both have ethical ramifications. What data can be collected is very different from what data should be collected. Disregarding the latter question can be more profitable, but doing so can often involve unethical practices and more importantly, compromise the privacy of individuals. It has become widely known that private enterprises collect all manner of (BI) data about individuals, causing ethical concerns. The ethics of privacy do not affect private enterprises alone. In recent times the development and implementation of public information systems by public agencies have also resulted privacy breaches, both overt and inadvertent. This is despite the fact that governments have a responsibility to protect private data from external parties. While some privacy laws have been enacted, paradoxically, other governmental legislation such as the Freedom of Information Act (FOIA) has actually eased restrictions on the very information that the privacy laws have sought to protect. In this context, it is useful to compare US privacy regulations other countries, e.g. Canada. It is also useful to contrast federal regulations with those in States, e.g. Connecticut. Ethical concerns regarding private information have also spawned various "solutions" whose motives and success can be widely interpreted. It can be argued that the protection of privacy and private information are the responsibility of both private and public entities, who should take concrete steps to classify and protect private information.

Keywords: Business intelligence, ethics, data collection, Freedom of Information Act, decision-making, Consumer Privacy Bill of Rights, privacy, confidential information

INTRODUCTION

Business Intelligence (BI) involves the collection of data; translation of the data into information; and interpretation of the information to help in decision-making. The goal of Business Intelligence is to make more informed decisions within an organization. For private businesses, these decisions translate to reducing waste and increasing profit. For governmental (public) agencies, these decisions translate to increased transparency and enhanced citizens' services.

However, while the goal of BI might be to make better decisions, it can also come at the expense of violating ethics – especially the ethics of privacy. Ethics is defined as a system of moral principles, based on which common laws are created in society. However, an unethical act does not necessarily make it illegal. Businesses seek to gain an advantage by sometimes using information unethically, though not necessarily illegally. Even government agencies have at times exposed private information under the guise of transparency – an act of questionable ethics.

Given the Internet's pre-eminent status as a premier communications tool, Internet privacy is of great concern in today's world. Average Internet users do not want their personal information to be exposed, especially if it is likely to cause financial or physical harm to them. Yet every Internet user has a different ethical notion of what sorts of information are considered private, and what are not. Because of this lack of clarity, businesses and governments need to explain to their users what their privacy policies are, and allow people to make choices on whether to use a particular service. Problems usually arise when businesses and governmental units assume that they have a legal right to information from users, and thus disregard privacy concerns.

In this paper we show how businesses and governments gather information, set rules as to how this information is used and accessed, and how that converges to or diverges from current ethics-based laws. We discuss laws that have been or are being created to handle the ethical and privacy concerns resulting from BI. We discuss cases where the allure of profits, or the reliance on BI was so great that businesses chose to violate their own terms of their privacy policies. We cite examples where businesses and governments gather information from the unknowing public. We compare federal laws and regulations with State laws and compare US laws with that of neighboring Canada. We conclude by providing an analysis of BI and privacy, and provide some suggestions on how to harmonize the two.

BI, ETHICS AND THE INTERNET

Internet Data Collection for Commercial Purposes: Who Collects it and Why?

The Internet has changed the way businesses target their marketing efforts. Instead of running billboard ads, print ads, and commercials on radio and TV, businesses can now market directly to users' computer screens as they navigate the Internet. Users, through their navigation patterns, leave behind a "trail of cookies" that marketers then collect and study. It is through these patterns that businesses develop strategies to tailor advertisement to users.

Internet browser "cookies" were invented in 1994 by Lou Montulli for the Netscape browser. They were intended to be the "eyes and ears" of digital store fronts, similar to an attentive shop keeper in a brick and mortar store (Singleton, 2000). Other methods that web based businesses use to track users include: click-tracking logs of all user navigation, form data submissions, and server requests logs that track information such as the IP addresses of users, date and time stamps of their actions, as well as the name of their operating system and Internet browser.

A variety of cookies called *third party cookies* are often used by businesses to track user behaviors, but their usage remains extremely controversial. These cookies are placed on a user's computer by a Web page they've visited, but not by the company that created the Web page. These cookies are developed by third party companies which specialize in tracking users' movements throughout the Web and use that data to deliver customer-specific advertisements. Once this cookie is placed on a user's computer every site he/she visits can potentially be recorded by this third party, especially sites that subscribe to the third party's service. The objective is to enable the third party to deliver relevant advertisements to Web users through their member Web sites.

Virtually all electronic retailers, search engines, and social networking sites also use some form of *click behavior tracking.* Never before has such an accurate portrayal of customer habits been available to retailers and advertisers. While this provides a benefit to businesses in that they can better target their advertisements, it can also lead to unethical practices in the way some marketers use the information they receive from this type of tracking.

Businesses, Information Collection and Privacy: Amazon.com

Amazon is one of the most successful retailers on the Internet. It has an extensive privacy policy which details how they capture information from their visitors. In the very first line of its privacy policy statement, Amazon states that merely by visiting their Web site a user is agreeing to the policy. There is no explicit means by which a user can "opt-in" or "opt-out" of their basic policy ("Privacy Policy," 2008). In its policy, Amazon states that any information the user provides it, and any information generated by cookies such as how long a user spends on each page, is recorded and logged. Amazon suggests that if any of their users do not want such data collected, they should refrain from filling out form data, or turn off personalized advertising within Amazon's site options, or disable cookies from within their Internet browser.

Amazon's privacy policy does not fully address how it uses the data collected from visitors. The only way for a user to opt out, other than never visiting Amazon's site is to block some of the Web site's elements from loading by changing his/her Internet browser settings. However, even this will not guarantee that Amazon will not receive the same information from third parties tracking Web users on sites other than Amazon.

Amazon is a retailer and understanding its customers is vital to its success. The limited option each user is given to opt out of the data collection suggests Amazon believes it can maintain its user base regardless of how their privacy policy is written.

How is the Collected Information Used?

To find out how the data collected by Amazon is used, Ghostery, a company which develops Internet browser plugins that "tracks the trackers", was used to identify how a user is tracked while visiting Amazon.com. It was found that a visit to the Amazon home page yielded six different third party tracking devices ("Applications Results," 2012). The following six trackers are tracked by the plugin: Admeld, DoubleClick, Millard Brown, OpenX Limited, Mediaplex,

and Microsoft adCenter. Each of these trackers monitors the Web activity of the user, for the duration that they maintain the cookie; if the user removes the cookie, the cookie doesn't begin recording until it is again downloaded from a page holding it. In doing so, it determines, from a pool of subscribing clients, what clients' products or services match the interests of the user based on their Web activity, and shows advertisements to the user for those products and services.

What is even more revealing is that while Amazon's privacy policy allows third party tracking, based on statistics issued by Ghostery, Amazon is just one of many Web sites contributing to the tracking of users through these third-party trackers . With the One Click tracker, information is shared between a minimum of six different tracking companies who correlate each user's information with the other users' information on hundreds of thousands of Web sites. In their study, Ghostery sampled Web sites relating to news, finance, sports, comics, pornography, weather reporting, databases, and social networking. While Ghostery's sample was relatively small, the categories of Web sites they chose creates a powerful picture of a Web user because on most of these types of Web sites users receive or post information. According to DoubleClick, another tracker, trillions of data points are updated every three to four hours to provide an up to date view of advertising performance ("Introducing new DFA," 2010). The primary goal stated in the description of each tracking company is to provide data to marketers so that they can better target their advertisements.

What Are the Rewards?

The Internet is a thriving marketplace of ideas and products. Its adoption continues to grow rapidly. It averaged 500% in worldwide growth from 2000 to 2011. The growth of the Internet in developing regions such as Africa and the Middle East is four times greater, topping 2000%. The worldwide Internet user base now is estimated to be 2.67 billion users, representing more than one third of the world's population (Miniwatts Marketing Group, 2012).

Getting the attention of all those users is a profitable business. According to the Internet Advertising Bureau (IAB), third quarter 2011 Internet advertising revenues are up 22% from one year ago. "Brand marketers recognize that their messages need to be where their consumers are spending their time, and that is increasingly in digital media" (Internet Advertising Bureau, 2011). Internet advertising giant Google racked up $36.5 billion in advertising revenue in 2011, representing 29% growth from the previous year and 97% of their total revenue ("2001 Financial Tables," 2012).

A Forrester Research study uses trends in monthly retail figures from the US Census Bureau to estimate the growth of e-commerce in the United States. The projection suggests online retailing will grow from 7% of total retail sales in 2011 to 9% in 2016. The spending increase is estimated to grow from $202 billion in 2011 to $327 billion in 2016, representing a 62% increase (Vertical Web Media, 2012).

Because it is financially beneficial to the development of e-commerce for users' Internet activities to be tracked, this motivation for companies to track a user's every move can spawn

many opportunities for unethical behavior, both in deciding what data should be collected and how that data should be used. Profit is the primary concern of a private business, and because the Internet affords businesses great power in tracking their visitors, their motivation to generate profit may outweigh their responsibility to behave ethically.

ETHICAL PROBLEMS AND EXAMPLES

Privacy Issues in Data Collection

In the U.S., the Privacy Act of 1974 provides the main controls within federal government on the collection, use, and disclosure of personally identifiable information. The law was designed to protect individuals from an increasingly powerful and potentially intrusive federal government (Subramanian & White, 2012).

"You have zero privacy anyway; get over it," said Scott McNealy, of Sun Microsystems in 1999. As the years have progressed technology has increased the ability to collect personal and private data from users. It will be up to businesses to use this collected information in an ethical manner. The question should be less about what they can collect and more about whether they choose to collect the data or not.

As previously discussed, user information of all types is collected, correlated, and modeled in ways Internet users cannot predict or comprehend. Privacy policies have been crafted with the company's ability to profit while trying to show concern and safety for each user's data. In order for users to experience all that the Internet has to offer, some data collection is necessary. One cannot place an order online without providing a name, shipping address, and some form of payment. Privacy cannot be about blocking all forms of data collection because all forms of Internet interaction would cease to exist.

Privacy issues on the Internet have been brought to the courts since its first commercial use. The first case involving the Federal Trade Commission was in 1998. In *FTC vs. GeoCities*, the FTC charged GeoCities, a popular Web hosting site, with misrepresenting their reasons for collecting personal information on children and adults. This had to do with the registration process and information that was freely supplied by users. GeoCities' policy stated that the information collected was only to be used to target advertisements of products and services to users and would not be shared with third parties. This information included questions about one's level of education, income, marital status, occupation, and other interests. The courts found that Geocities did in fact provide this information to third parties, violating their own privacy policy (Federal Trade Commision, 1998)

Another case, *Raytheon vs. Yahoo* in 1999 involved employees of Raytheon who used Yahoo! groups to communicate. Some employees disclosed confidential information using this forum. They believed their posts were anonymous because they did not use their real names. The users expected Yahoo! to protect their privacy and not to supply their real names. However, when faced with a subpoena Yahoo! gave up the users' identities to Raytheon resulting in 21 of them

being sued for discussing corporate business on a public platform. Yahoo!'s policy at the time was not to sell or give away users' information, however in this instance they were forced to do so by court order. (Associated Press, 1999).

Internet privacy decisions span from data collection to the proper usage of the data obtained. Some decisions are risky, especially when they involve a company circumventing its own privacy policy just so that certain information can be collected. Companies willing to breach the public's trust are risking loss of their company's reputation while opening themselves to civil and criminal prosecution. At the same time, Internet users expect anonymity, and as a result, do not exercise vigilance in protecting their privacy.

Examples of New Data Collection Practices and their Impact on Ethics and Privacy
Google has become synonymous with Internet advertising and data collection. In 2012, Google had 85% of the search engine market share as shown in Figure 1 (Netmarketshare, 2012). Google's expressed motto is "Don't be evil." The "evil" mentioned refers to betraying the high ethical standards it has set for itself. The following is Google's preface to their Code of Conduct:

"'Don't be evil.' Googlers generally apply those words to how we serve our users. But 'Don't be evil' is much more than that. Yes, it's about providing our users unbiased access to information, focusing on their needs and giving them the best products and services that we can. But it's also about doing the right thing more generally -- following the law, acting honorably and treating each other with respect" ("Code of Conduct," 2009).

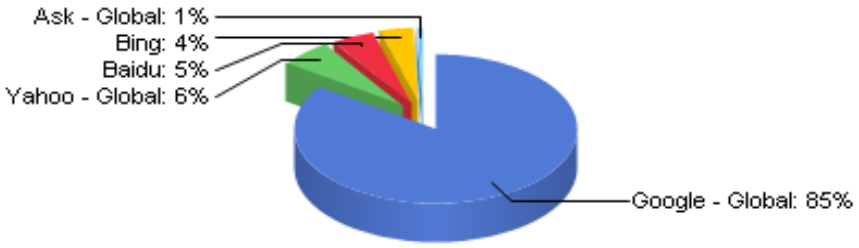

Figure 1: Pie chart of Total Market Share of Search Engines (Netmarketshare, 2012).

This admirable statement reflects a simple position on being ethical. Google does not believe in using loopholes to gather information, instead they follow a simple, down to earth philosophy in making ethical choices. The policy goes on to show a commitment to advancing privacy for users around the world. The policy became part of the company's reputation as a group of do-gooders out to improve the world while representing an alternative to original corporate search engines by Yahoo!, Microsoft, and America Online.

While Google has built a reputation based on following its own motto, recent investigations have found ethical lapses that could tarnish Google's reputation. A report in *The Wall Street Journal* indicates Google recently used coding tricks to collect users' information from those using

Apple's Safari browser (Angwin & Valentino-Devries, 2012). Google placed code to "exploit a loophole" in the Safari browser that tricked it into thinking a user was submitting form data, the only way that the browser is allowed to collect user data, according to Apple's privacy policy for the browser. In essence, Google faked the Safari browser into allowing Google to track users' activities despite their expectation of privacy. According to the journal, Google stopped this policy once it became public. If the FTC investigates and finds Google guilty of breaking previous privacy agreements, the fine would be $16,000 per incident (Halzack, 2012).

Google's tactics in this example are certainly a prime example of unethical practice. Google figured out it could collect data from Safari users, but the decision to do so should have included some consideration of the impacts. These types of actions are likely to chip away at Google's reputation, and could potentially cause a loss of market share, and spur litigation and fines. It would set a terrible precedent if Google goes unpunished, because if they can exploit loopholes, why can't others? Further, how can a competitor compete with a market leader who makes their own rules and chooses when it is convenient to follow them?

An account of Google's infiltration of the Safari browser appeared in the Washington Post and summed up the reason why we will continue to see this type of ethical boundary tested or broken. "The secret to winning the future of the Internet lies in the ability to monetize all this personal data. This is especially true, now that many people are shifting their Web consumption habits to mobile devices, which theoretically enable real-time, 24/7 tracking. At the end of the day, Web firms need your data for essentially two reasons: (1) to deliver a more personalized experience for users or (2) to sell this data to advertisers and third parties. Thus far, we've given companies like Google a free pass, taking them at their word that they are not somehow 'evil,' that they are, indeed, delivering a superior, personalized experience" (Basulto, 2012)

The Internet's most popular social networking site Facebook has been under scrutiny for its privacy policies. The company recently settled with the Federal Trade Commission over several cases where Facebook failed to keep its promises of privacy to its users through frequent changes to its policy and site structure, thus making it too confusing for the average user to understand. The proposed settlement bars Facebook from making false claims about privacy practices and requires they give users a minimum amount of time to adjust to changes in a privacy policy. Facebook will also have to accept 20 years of independent third party monitoring of its privacy practices. Any violations found may result in a civil penalty of $16,000 per charge (Federal Trade Commission, 2011).

SOLUTIONS TO ETHICAL PROBLEMS IN INTERNET COMMERCE

Government Solutions

Driven by consumer complaints, governments have been compelled to act. When unethical behaviors affect a large population they tend to react and pursue punitive litigation and preventive legislation. The Obama administration has unveiled what it calls the "Consumer Privacy Bill of Rights". This bill of rights is designed to protect Internet commerce by protecting

Internet companies from themselves. This bill would use a third party to protect user privacy through regulations. These new regulations would be enforceable by the Federal Trade Commission and are designed to be a framework for legislation. One of its goals is a free and open Internet without global borders. While a grand goal, it would detract from the primary goal of protecting consumers. It is not entirely possible for the Bill's reach to expand to the entire globe because different countries have different laws and regulations on Internet usage and transmissions.

The bill stresses that industry leaders should determine the rules while maintaining a certain level of flexibility for innovation. The bill calls out specific Internet browser providers to make a "do not track" feature that allows users to have a choice when it comes to privacy (The White House, 2012). For example, Google's Chrome browser allows this through its "Incognito" feature.

The bill of rights would protect consumers in the following ways: individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability. While this proposed bill of rights doesn't start with the strength of law, it does address the major abuses Internet consumers have suffered, including false statements in privacy policies and exploiting technology to circumvent those policies. Those practices have resulted in information being spread beyond the intended boundaries, as in the cases discussed with Facebook and Google. It is possible that creating such laws would be difficult up against the huge profits in a society that values money above all else. In any case it appears to be a good start at the federal level.

State governments have also enacted laws to protect users' privacy on the Internet. California has laws that prohibit any type of monitoring of email, chat, or e-book reading while using library computers. California also prohibits revealing information about books selected or pages browsed from any electronic source including online booksellers. Minnesota requires that Internet service providers get permission from subscribers before disclosing information about surfing habits. Connecticut and Delaware require employers to notify employees before reading their emails, or monitoring their Internet access. California, Connecticut, Nebraska, and Pennsylvania have laws requiring a posted privacy policy and or prohibited any false statements in a privacy policy. Sixteen states require government Web sites to have privacy policies (National Conference of State Legislatures, 2012). The state laws are much narrower than the Federal Bill of Rights and seek to correct a specific wrong.

The State cases researched seem to focus on privacy in the context of those using public resources and employee rights. The Connecticut Law example imposes a $500 fine for each instance of monitoring by an employer of an employee's electronic communications without notification of the monitoring. This law protects business more than employee privacy. Once the business has notified the employee of monitoring, the business is generally free to continue to monitor the employee. Only the ignorance of the law results in a problem for a business that chooses to monitor employee communications.

Industry Solutions

Recently, some "industry solutions" to protect an Internet user's privacy have emerged from various Internet businesses. However, even these will most likely be driven by monetary aspects just as the past abuses have been.

A recent example of this type of industry solution is Google's "Circles" feature of Google+. It allows the user to group their friends into categories and set permissions regarding what type of information each group can access. For example, a user may want close friends to have access to everything but co-workers access only to contact information ("Privacy Policy, 2012).

As of March 1, 2012 Google implemented a new privacy policy which includes some important changes that speak to many privacy concerns previously raised. Google claims that the policy provides greater transparency to the user and allows them to *choose* through the Google Dashboard what services within their Web site – of which there are many – they are allowed to collect and maintain user data ("Real-Life," 2012). Further, Google initiated an opt-in process for the sharing of user information with outside companies and organizations; one's personal information cannot be shared unless the user consciously opts in, by default no action is taken and the user does not need to opt out.

These changes address some important privacy concerns. It gives users and the ability to determine what data Google collects about them and additionally allows users to make changes to how that data is collected and used. It also allows users to remove some of the information that is collected and stored over time. This represents a major change from the typical industry attitude, which provides the user almost no control over what information is collected or how it's used. The "Information We Share" section has an interesting provision. It indicates Google will require users to "opt-in" before sharing sensitive personal information or SPI. Sensitive personal information is described by Google as: confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality. This type of information (lifestyle, medical, origins and beliefs) in the wrong hands can be used to harm or harass. Its protection is very important. The required opt-in is a step in the right direction to reduce its misuse

OPT-In vs. OPT-Out

Google's decision to go with an opt-in model vs. opt-out model is important. Opt-in requires a user to permit the Web site to collect and use information in a certain set of ways before the collection of that data ever begins, whereas the opt-out system allows the Web site to behave however the designer wants by default unless the user takes action and opts out of the default settings. When a choice is given it is often to opt-out. This gives the operator implicit approval to share information. Consumers generally do not opt-out possibly due to laziness or ignorance. A Gallop survey showed 67% of US Internet users disliked targeted advertising but only 37% would choose to opt-out (Hatch, 2012). The opt-in model forces internet users to make a choice and possibly even think about the repercussions of that choice. To go to an opt-in model for all Internet data collection would be tedious but useful. Perhaps a clear and simple interface that breaks the information into a few clear distinct categories would make going to an opt-in model

more palatable. In any case even a small move toward opt-in such as Google's new SPI privacy policy is a step in the right direction.

The Network Advertising Initiative (NAI) is an industry attempt at addressing online privacy. The network consists of a coalition over eighty online advertising companies that have agreed to a self-regulating code of conduct. Some of the largest Internet advertisers have joined, including Akamai, AOL, Google, Yahoo! and Microsoft. One of the goals is self-imposed restraints among members to achieve a balance between consumer confidence and the ability to continue to use third party data collection to create the business intelligence to effectively market products and services to them. The initiative includes numerous straight-forward provisions for the behavior of advertising companies related to how they use data from Internet users. The provisions represent an ethical framework from which to operate from. The NAI also provides a tool to opt-out of behavior based advertising from coalition members. The tool works by placing a cookie in the Web browser that prevents targeted advertising. The cookies do not expire for five years. The tool allows users to opt-out from individual trackers and even indicates if there is an active tracker already stored in the user's browser (Network Advertising Initiative, 2010).

The Network Advertising Initiative, which exists as an ethical guidebook to preserve consumer confidence, been widely accepted by many industry leaders, is proof that a problem in this area has been recognized. It is in the industry's best interest to self-police, such as this, to slow or prevent pressure for lawmakers to act in ways that may limit their ability to expand and innovate.

Individual User Solutions

The legal and regulatory environment appears to be in the early stages of development, wherein individual users cannot rely on the industry or government to protect them. Thus it is imperative that users exert pressure on the government to improve the situation. However at present, the solution seems to be to understand the environment and take steps to protect one's own interest. As previously shown, the financial rewards to the industry are so great that ethical lapses are the norm rather than the exception. Awareness of what users are giving away and how it may be used along with the techniques to limit its spread is the best solution that is currently available. The Electronic Frontier Foundation attempts to educate Internet users on protecting their online privacy. The recommendations include common sense advices such as "Do not reveal personal Information inadvertently" and "Don't reveal personal details to strangers or just met friends". They also include technical discussions related to cookies and encryption (Electronic Frontier Foundation, n.d.).

The technical details of cookies and encryption are difficult for many Internet users to understand. A wonderful thing about an unrestrained Internet marketplace is that if there is a hole in the needs of consumers someone will attempt fill it. There is a new and growing category of software in the form of browser add-ons that help make it easier for consumers to wrestle back control of who gets their information. The previously mentioned Ghostery is one of half a dozen browser add-ons offering to take on the technology piece of privacy protection for the user.

The Internet privacy environment is beginning to show signs of improvement. However, the rewards still far exceed the penalties when it comes to unethical behavior related to the use of data collected on the Internet. The information and the tools are available but it's up to the users to decide whether or not it's worth the effort to use them to protect their privacy.

BI, ETHICS AND THE GOVERNMENT: *HOW FAR SHOULD DATA COLLECTION GO?*

Government Data Collection: Is Sensitive Data Collected and Why?

Data are collected at virtually all levels of government—federal, state, and local—to enhance administration and decision-making, as well as to make certain aspects of government, namely use of taxpayer dollars, more transparent. The accurate collection, maintenance, and sharing of data between each level of government leads to better decision-making.

In the United States, an E-Government Task Force was established in July 2001, to "identify priority actions that achieve strategic improvements in government and set in motion a transformation of government around citizens," (United States, Executive Office of the President, 2002) according Mark Forman, Associate Director for Information Technology and E-Government.

The responsibilities of this task force are to identify strategic opportunities for e-government. To that end, 71 interviews were conducted with over 150 senior government officials. Consensus was that there is a growing desire for government agencies to use the Internet to help provide its services, whether those services are benefit related, recreational, or educational. Further, there is a desire among government entities at each level of government to share and integrate data between federal, state, and local databases. Ultimately the goal that most government officials seek is to streamline their processes by adopting commercial best practices to reduce their operating costs and simplify job duties in finance, human resources, procurement, etc.

G2C • Use the web for accessing services such as benefits, loans, recreational sites and educational material • Key lines of business: social services, reaction and natural resources, grants/loans, taxes	**G2G** • Reduce burden on businesses by adopting processes that enable collecting data once for multiple uses and streamlining redundant data • Key lines of business: regulation, economic development, trade, permits/licenses, grants/loans, asset management
G2G • Share and integrate federal, state and local data • Key lines of business: economics development, recreation and natural resources, public safety, law enforcement, disaster response management, grants/ loans	**IEE** • Adopt commercial best practices in government operation (supply chain management, HR document workflow) • Key lines of business: supply chain management, HR, finance

Figure 2: Goals of the United States E-Government Task Force (United States, Executive Office of the President, 2002).

Distinguishing Between Necessary and Excessive Data Collection?

There is a growing concern among individuals that government entities are collecting too much information about their citizens. In Figure 2 above, we see types of data that is frequently collected by each federal agency and made available for statistical analysis, but sometimes, data pertaining to specific individuals is collected for no outwardly apparent reason. While it is clear from the previous section of this paper that certain data sets are critical for better decision-making and streamlining government operations, there remains a risk that some agencies will take data collection too far. In many cases, drawing the line between what is necessary and what is excessive is a decision that is ultimately made by the court system.

Examples of Questionable Data Collection

On January 23, 2012, the United States Supreme Court ruled in United States v. Jones that it is unconstitutional for authorities to secretly place a Global Positioning System (GPS) device on a person's physical property to track their location over time (Hentoff, 2012). In the particular court case, a law enforcement agency secretly planted a GPS device on the defendant's vehicle, without him knowing, however the court's ruling in itself will set a precedent for all similar situations (ex. An agency planting a GPS device on someone's clothing). While this was celebrated by most of the public and the media, there remained concern by some that government agencies still can, and frequently do, collect massive amounts of similar data without necessarily *physically* intruding on them. Thus, they are still able to collect data such as that in this court case, but through other means such as surveillance technology. Surveillance technology, in particular, has evolved rapidly over recent years, both in the technology itself and its use by government authorities.

In response to the court's ruling, John Whitehead of the Rutherford Institute pointed out that between the use of facial-recognition software, biometric analysis, Radio Frequency Identifications (RFIDs), and giant databases to track and categorize data generated by these and other emerging technologies, often recorded without warrant, the privacy of individuals is often breached without their knowledge. Thus, they have no ability to file a constitutional complaint as the defendant in this case did because they aren't even aware of it occurring. Further, if manufacturers or clothing distributors begin to tag their clothing with RFIDs and law enforcement personnel begin using RFID readers, they could easily track you without you ever knowing. Even when there exists a law or court-set precedent regarding privacy, one has little recourse when they are unaware that their personal privacy has been breached. In addition, Mr. Whitehead points out that the actions taken by the law enforcement personnel in this court case are still legal in many states so long as an officer has a mere *suspicion* of the individual's involvement in a crime.

Sometimes data collection and even publication that breaches one's personal privacy rights has nothing to do with law enforcement. For example, the U.S. Department of Agriculture collected and publicly listed the social security numbers of thousands of their financial aid recipients. While the social security numbers did need to be collected, obviously they did not need to be made public, and the most chilling part of this disaster is that the department was completely

unaware their public database even showed social security numbers until the state of Illinois reported it to them.

Legality of the Government's Data Collection

The federal Government Accountability Office (GAO) gave testimony in 2008 after assessing the "sufficiency of laws covering the federal government's collection and use of personal information," (United States Government Accountability Office, 2008a) and found that many aspects of the Federal Privacy Act's protections are outdated and do not apply to modern IT infrastructures, which change at such a rapid pace that policies governing them cannot seem to keep up. The GAO strongly recommended that Congress revise the scope of their federal privacy laws to address these issues, so as to limit both what the federal government can collect and *how* they can use the information that they do collect (United States Government Accountability Office, 2008b).

In their review, the GAO looked at the Federal Privacy Act, the E-Government Act, and guidance issued by the Office of Management and Budget (OMB), and found major inconsistencies in the way that privacy requirements for agencies attempt to protect personally identifiable information. There were three areas of greatest concern that the GAO had in their review of the legislation (United States Government Accountability Office, 2008a):

1. **Applying privacy protections consistently to all federal collection and use of personal information.**

The scope of the Privacy Act is limited to what it defines as a "system of records," and the definition varies between private entities and federal agencies. Sometimes the same record, if collected by the government as opposed to a private entity, would not be within the scope of the Act, but would be if it were collected by a private entity. The definition of what falls into the law is not consistent between the federal government and commercial enterprises.

2. **Ensuring that collection and use of personally identifiable information is limited to a stated purpose.**

Especially in the post 9-11 era, it is widely recognized that agencies need to better coordinate and share data with one another, however the GAO is concerned that sharing between government agencies may at times be excessive, requiring policy that aims to balance the justification to collect and use certain information for specific purposes and establish agreements between agencies before any data sharing occurs.

3. **Establishing effective mechanisms for informing the public about privacy protections.**

The public is often left in the dark about the government's policies regarding what can be collected, how it can be collected, and how it can be used, or are given vague summaries to that effect. The GAO believes the public is entitled to greater detail on this issue, and that the Internet should be used to do distribute such information.

Figure 3 outlines some of the most common sensitive information maintained by governments and the current laws governing their collection, use, and publication.

Information covered	Applicable law
Patient health information	To the extent a federal agency is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), e.g., a provider of health care programs or services, it may not use or disclose an individual's health information without the individual's authorization, except for certain reasons, and is required to inform individuals of its privacy practices. 42 U.S.C. §§ 1320d – d-7; 45 C.F.R. Part 164.
Statistical information	The Confidential Information Protection and Statistical Efficiency Act (CIPSEA) requires that information acquired by an agency under a pledge of confidentiality and for exclusively statistical purposes shall be used by the agency only for such purposes and shall not be disclosed in identifiable form for any other use, except with the informed consent of the respondent. Sec. 512, Title V, Pub. L. No. 107-347, Dec. 17, 2002; 44 U.S.C. § 3501 note.
Census data	Except as specifically authorized by law, the Census Bureau may not disclose identifiable census data. Penalties of up to $5,000 and 5 years in prison apply for violating the law. 13 U.S.C. §§ 9 & 214.
Taxpayer data	The IRS must keep taxpayer information confidential and may only disclose it under limited circumstances, e.g., for federal or state tax administration, to assist in the enforcement of child support programs, to verify eligibility for public assistance programs, and for use in a criminal investigation. Individuals or agencies receiving taxpayer data must, as a condition of receiving such data, have safeguards for the protection of, and for accounting for, the use of such data. 26 U.S.C. § 6103.
Social Security information	Social Security numbers and related records must be treated as confidential and may not be disclosed, except as authorized. 42 U.S.C. §§ 405 & 1306. Such other authorized uses include disclosures for bankruptcy proceedings (11 U.S.C. 342(c)), enforcement of child support programs (42 U.S.C. §§ 653, 653a, & 666(a)(13)), and enforcement of immigration laws (8 U.S.C. §§ 1304 & 1360).

Figure 3: Types of Data Visible on Federal Agency Websites and Applicable Laws
(United States Government Accountability Office, 2008a)

US and Canadian Data Collection: Comparison

The United States is not alone when it comes to public concern over government data collection. In February 2012, Bill C-30 was proposed as a federal Canadian law which would require Internet Service Providers (ISPs) and cell phone companies to immediately share customer information with law enforcement personnel without a warrant. According to Adrian Humphreys, writer for the *National Post*, this bill is nothing new in Canada, and indeed, one's "data shadow" is already "huge" (Humphreys, 2012).

The Canadian government has experimented with automated license plate readers, biometric recognition of faces in surveillance footage using driver's license photos, and performing statistical analysis using health records, income, and spending habits. Michael Vonn, policy director of the B.C. Civil Liberties Association, notes that "The government has a voracious appetite for our private information. Now, with electronic records, we do that by linking electronic databases without ever creating the actual, old file. It's already there." He further states that "… the growth of the database nation presents a grave danger to democracy."

IMPACT OF TRANSPARENCY LINITIATIVES

The Freedom of Information Act (FOIA)

Consistent with the founding fathers' general mistrust of a central government in the early years of United States' history, today it is deemed sound public policy for United States' citizens to be able to monitor government activities. To that end, Congress passed the Freedom of Information Act (FOIA) in 1966, which mandated, upon request, the disclosure of most federal information to any citizen. The intention of the FOIA was to prevent agencies from holding tight information regarding their operations that might cause public scrutiny if those operations or activities were known by the public (Montana, 1998). The United States is not the only country to have freedom of information (FOI) laws. Sweden has had, in some form, freedom of information laws going back to 1766. Canada, Australia, and New Zealand passed FOI laws in 1982. Ireland passed its freedom of information act in 1998 and the United Kingdom soon followed in the year 2000. In addition, Denmark, Holland, Norway, and Hungary all have FOI laws. FOI legislation is most certainly not an American phenomenon; there is a global desire of people to develop an awareness of what their government is doing (Frankel, 1998).

The FOIA of the United States requires all records of federal agencies, including those that are electronic, to be disclosed upon request unless they fall into the following types of information as shown in Figure 4:

a. **Exemption 1**: classified national defense and foreign relations information

b. **Exemption 2**: internal agency rules and practices

c. **Exemption 3**: information that is prohibited from disclosure by another federal law

d. **Exemption 4**: trade secrets and other confidential business information

e. **Exemption 5**: inter-agency or intra-agency communications that are protected by legal privileges

f. **Exemption 6**: information involving matters of personal privacy

g. **Exemption 7**: records or information compiled for law enforcement purposes, to the extent that the production of those records (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions, or (F) could reasonably be expected to endanger the life or physical safety of any individual

h. **Exemption 8**: information relating to the supervision of financial institutions

i. **Exemption 9**: geological information on wells

Figure 4: FOIA Exemptions (United States Department of State, 2011).

There is no limitation with respect to who may request government records under the FOIA. Agencies must respond to requests filed by "any person," according to the Act (Montana, 1998). This extends to corporations and other legal entities because, in law, they are considered "persons." A wide variety of parties have utilized FOIA to gather information, not just ordinary private citizens, but special interest and advocacy groups, commercial organizations, news organizations, and authors.

Agencies have ten days to respond to a request, and an additional ten days beyond that if there are "unusual circumstances." If the agency believes the requested information qualifies as one of the previously outlined exemptions, or has grounds under which to deny the request, they may do so, but the requester can appeal that decision, and if they do, the agency must respond to the appeal within twenty days. While these deadlines are quite strict, there have been times where courts have excused the noncompliance of agencies in meeting those deadlines. If it was beyond the control of the agency in meeting the deadline, then the courts usually cite that as a reason in excusing the agency from not having met the deadline. However, with these deadlines in place, agencies cannot simply ignore the deadline, as the requester can bring the matter to court.

Agencies may charge the requester fees for time spent on the request and expenses, such as making copies of the requested items, however there are legal limitations as to how much can be charged relative to what is requested. In addition, agencies must "make a reasonable search for records pursuant to any reasonably specific request, using methods reasonably calculated to produce the requested information" (Montana, 1998). While this language is somewhat vague and open to judgment, agencies cannot just claim that it is "too hard" to fulfill a request simply because they don't want to, as if the matter is brought to court, they must defend that assertion.

FOIA has led to a massive increase in the amount of public information regarding government operations, and much more accountability of government activities. Journalists and news organizations have discovered and exposed illegal, embarrassing, and frowned upon activities at virtually every level of government. In many cases, information revealed through FOIA requests has revealed what many believe to be unethical collection of information, or surveillance, by government authorities. Ultimately, these discoveries and public disclosure have led to major reforms in what types of personal information the government is legally able to collect about people.

There has also been some abuse of the FOIA system. While there are many good things that have come from the FOIA, there have also been some unintended consequences. While there are many good reasons to utilize the FOIA to request certain information, citizens may use it for, quite literally, any imaginable reason. As a result, there are times when agencies must sacrifice significant time, money, and resources, to fulfill a FOIA request, regardless of who is requesting the data or what their reason might be. While courts recognize this and excuse tardiness in meeting the FOIA deadline for requests that are large or are unreasonable to expect completion in a mere ten days upon receipt, government agencies can still get bogged down by the number of FOIA requests they receive and the pressure by the deadlines of the Act and the natural tendency of the court system to enforce them unless there are reasonable grounds for a longer deadline. What many label as true abuse of the system is when a company that is in the business

of selling information – a large and growing industry – requests information from a government agency, for example a list of licensed drivers or registered voters, and then chops it up into pieces and sells each piece to interested parties. For example, a business might request a list of all registered voters in a state and then divide the list into lists by town, and sell it to parties from each town who are interested, for a fee, making an overall profit, all at the expense of the government's time and money putting the data together and releasing it to the requester under the FOIA. The time spent on fulfilling such a request could have been spent catching criminals, fighting terrorism, or other important goals, but in cases such as these, is literally spent transferring wealth to private enterprise (Montana, 1998).

State legislation expanding upon the Freedom of Information Act

Many states have passed transparency initiatives which expand upon the FOIA by actually publishing information on the Internet that is frequently requested by the public. This promotes government accountability and, in the long run, can cut down on the amount of time spent fulfilling specific FOIA requests that collectively fall under the same broad category (ex. State government spending, employee salaries, pension amounts, etc).

The State of Connecticut is a great example of this. Public Act 10-155 was approved by the Connecticut General Assembly on June 7, 2010, and called for the Connecticut Office of Fiscal Analysis (OFA) to develop and make public an Internet Website with a searchable database that includes state expenditures, contracts and grants, state employee salary information, and state retiree pension information. It also called for each agency of the state receiving state funds through the budgetary appropriations process, as defined by Section 4-60 of the Connecticut General Statutes, to submit to the OFA any information it requests from them to achieve that end ("An Act Requiring," 2010).

Public Act 10-155 also called for a review by the Connecticut Auditors of Public Accounts to determine whether the database accurately reflects the data it is intended to summarize and provide and determine whether any of the information it provides infringes upon the right to privacy of any individuals employed by the state or contains any information that a state agency might consider confidential.

In the State Auditor's review of the database, it was found that the database contained detailed information for in-scope agencies and quite limited information for limited-scope agencies (Auditors of Public Accounts, 2011). In-scope agencies refer to those agencies that use the statewide accounting system known as Core-CT for accounting at the voucher level of transactions while limited-scope agencies account for transactions only at the level of the general ledger, among other differences in the level of interaction with the statewide system. In-scope agencies use the central system for all accounting, asset, and HR functions, while limited-scope agencies use the central system for some things but not others. Prior to the Auditor's review, the database did not include certain items from the limited-scope agencies and did not disclose that the data presented for limited-scope agencies was incomplete. Subsequent to the review, while the data remains incomplete, clarification regarding what data is excluded from the database has been added to the Web site. In addition, while the review did not determine any confidential

information was presented on the Website, no disclaimer existed indicating that some information, which agencies deemed confidential, was excluded from the database. The OFA accepted the Auditor's recommendation to add a disclaimer stating that certain information deemed confidential was omitted from the database.

Personal Reaction to Connecticut's Transparency Initiative

As an employee of the State of Connecticut, I (Brian DeMilia) was personally affected by the publication of Connecticut's Transparency Web site, http://transparency.ct.gov/. Many state employees thought of the Web site as an invasion of privacy. All of a sudden, any one of your coworkers, or any one of your family members or friends, could do an Internet search to determine your salary, and the composition of your salary. Many employees who clocked exceedingly large amounts of overtime towards the end of their career in order to inflate their three highest years of salary-contributing to their pension calculation became exposed to the public eye. News outlets used the Web site to comment on every embarrassing situation. Policies regarding tuition reimbursement also vary from agency to agency, as well as mileage reimbursement between each branch of government, causing some employees to be uncomfortable with others knowing how much they were getting reimbursed. In a private company, you would never have to worry about any person imaginable being able to look up your salary or the benefits you received, and some state employees thought they were entitled to that same level of privacy. However when taxpayer dollars are involved, that privilege goes out the window. And while it once took a FOIA request for the information to get out there, Public Act 10-155 literally made it as easy as an Internet search – with the data already out there – for everyone to see.

Designation of What information is Deemed Confidential

Because the Freedom of Information Act (FOIA) allows anyone to request any set of records from any agency, it is critical that agencies implement policies related to best practices in stamping or tagging, either physically or electronically, what records, or portions of records, are deemed confidential. Likewise, it is also critical that agencies maintain a list of what types of records are confidential and those that aren't. If a confidential record is not labeled confidential, and the preparer or collector of that record files it away without marking it confidential, if a FOIA request comes in and it is processed by someone other than the preparer, that person has no way of knowing that the document is indeed confidential. In turn, such a record, even though confidential, could be made public. Depending on the reason for the record being confidential – for example, showing social security numbers – the release of it could open up the agency to legal liability.

One of the authors, Brian DeMilia, works as a staff auditor at the State of Connecticut Auditors of Public Accounts and mentions how his office handles information:

As an auditor of Connecticut state agencies, working papers must be electronically tagged as confidential, where applicable, so that if a FOIA request calls for the release of them – which normally are not made public, only the resultant audit report – those particular pages would be

excluded from the release to the requestor. A separate employee handles the FOIA requests so there would be no way of knowing, nor would there be the time to examine, which files from an audit folder shouldn't be made public. This employee relies upon the distinction, upon preparation of each file, of what is confidential and what is not. If one was to miss a page that is confidential, and their supervisor was also to overlook it in their review, that page would be released upon a FOIA request. Depending on the magnitude of the error – what type of information was on the page – the impact could be disastrous.

Sensitive Versus Confidential Data, What is the Difference?

Sensitive information is information which an agency may deem inappropriate to release even though it may not necessarily be confidential. A good comparison of this is an employee's employee number versus their social security number. An employee's employee number is sensitive information, but it is not confidential. An employee's social security number is, however, certainly confidential, and must not be released through a FOIA request.

GOVERNMENT RESPONSIBILITY TO PROTECT SENSITIVE AND CONFIDENTIAL DATA

Government Employees' Misuse of Data

Who can forget "Joe the Plumber" and his role in Obama's campaign for the presidency in 2008? Samuel Wurzelbacher – this man's real name – became a national celebrity after challenging then candidate Obama's tax policies while he was campaigning in Mr. Wurzelbacher's hometown.

Shortly following Mr. Wurzelbacher's rise to fame throughout the nation, an unprecedented number of searches made by state and local government employees accessed his personal information (Provance, 2008). In response, the Ohio legislature sought two bills, one in the House and one in the Senate, which, if passed, would allow citizens to sue government employees who used government computer databases to get their information without just cause, and if the government employee weren't unionized, to have such action result in the employee's immediate termination. Senator Mark Wagoner, sponsor of the Senate bill, said "It was an abuse of Joe Wurzelbacher's personal privacy," adding that "Ohioans share confidential information with state government and expect it's only going to be used for its intended purposes. Here, that trust was abused" (Provance, 2008).

It was later determined by Governor Ted Strickland, through a review conducted by state Inspector General Tom Charles that Helen Jones-Kelley, director of the Ohio Department of Job and Family Services, that she, without just cause, authorized database searches for any potential public assistance, child support, and unemployment compensation records on Mr. Wurzelbacher. In response to her actions, Governor Strickland suspended her without pay for one month and also suspended two of her assistants for participating in that decision, as well as reprimanding two other employees who failed to safeguard the databases (Provance, 2008). Governor Strickland commented that while he disciplined his employees for accessing information without

just cause, there was nothing in the law making that illegal. However, under the two bills proposed in Ohio, governments would have to establish policies for when confidential personal information maintained in their database is accessed and would require individuals searching the database to declare their reason for each search. In addition, intentionally accessing and disbursing such information without cause would become a legal matter – a first-degree misdemeanor – punishable by up to 180 days in jail. This legislation was eventually signed into law by Governor Strickland on January 6, 2009, with an effective date of April 7, 2009 (Ohio Legislative Service Commission, 2009).

The State of Connecticut's central information system known as Core-CT is set up in a similar fashion in that tables holding sensitive human resource information are tagged and, when accessed through PeopleSoft Query, a comment line is added to the user's SQL statement indicating their username. While this does not apply to the limited few who have direct database access to write their own SQL, most employees who can only execute queries using PeopleSoft Query cannot actually write their own SQL and are only able to execute queries built using the PeopleSoft software. And because that software adds their username as a comment line to their query, logs of queries having been run will in turn allow, whenever needed, an investigation into who accessed whose information.

The United States is certainly not the only nation to see major abuses by government employees. Kathleen Karen Beggs, former employee of Canada's federal Department of Revenue, received four years in jail and a $30,000 fine for repeatedly defrauding the department (Hall, 2003). Beggs used her high security clearance to access and manipulate computer records to obtain fraudulent tax credits and refunds for herself and her friends. She pleaded guilty on May 24, 2002, to nine counts of fraud, one count of misuse of taxpayer information, and one count of tax evasion. In addition to her fine and imprisonment she was also ordered to pay restitution, which started at just over $221,000 but was ultimately reduced to $103,235.

Beggs used her security clearance to improperly obtain taxpayer information and override the change data in the database. She fraudulently created tax credits and refunds totaling $221,434.96 for herself, various family members, friends and acquaintances, under the Child Tax Benefit and B.C. Family Bonus programs of Canada (Hall, 2003). The eventual end to Begg's spree of fraud came when she refused to help a friend of a friend fraud the system. Upset, they contacted the authorities and informed them of Beggs' actions. In addition to the fraudulent money received, Beggs failed to report that money on her return, another offense which prevented her from having to pay an additional amount of $30,991.83 in taxes. The court, noting that Beggs managed to obtain a security clearance that is only given to the top five percent of employees at Canada's Department of Revenue, "badly abused her position of trust, not only to her employer, but to the citizens of Canada," said Appeal Court Justice Catherine Ryan.

Government Loss of Sensitive or Confidential Data

Perhaps one of the most notorious cases of government employees' loss of data in the state of Connecticut was the loss of a Department of Revenue Service's (DRS) employee's laptop in 2007, which contained the confidential personal information, including the names and social

security numbers, of over 106,000 state taxpayers. The employee, Jason Purslow, left the laptop in his car while in Islandia, New York, where it was stolen (Auditors of Public Accounts, Office of the Attorney General, 2009).

DRS ended up paying more than one million dollars to provide identity theft protection to affected taxpayers in order to remediate the data loss, and while no misuse of taxpayer information has been definitively connected the event, the whereabouts of the laptop remain unknown and the impact of the event may remain forever unknown and immeasurable.

Upon the theft of the laptop, the Connecticut Auditors of Public Accounts (APA) and the Connecticut Office of the Attorney General (OAG) received many complaints alleging DRS's mishandling of confidential taxpayer information that could result in the identity theft of taxpayers or misuse of that information. Additionally, many complained that DRS failed to adequately investigate the theft of the laptop.

In following up on these investigations, the APA and OAG performed their own investigations, which revealed significant deficiencies in DRS's policies and procedures concerning confidential taxpayer data. In their collection of evidence, they concluded that the theft was directly related to DRS's failure to implement effective security and tracking measures. In addition, they found that the particular laptop that was stolen should not have contained taxpayer information. The employee transferred it from his desktop to his laptop, which was not encrypted, without legitimate reason. It was also found that, because DRS did not immediately investigate the event, there was a five day delay before the matter was brought to public attention, leaving a five day window where taxpayers were highly exposed to identity theft and financial harm. Recommendations of the Auditors and of the Attorney General were that the DRS should:

DRS should train all employees to spot data breaches and teach them what to do if they happen. DRS should hold employees accountable if they fail to follow data breach protocols and procedures.

DRS should continue ongoing efforts to update its computer networks so that all confidential taxpayer information is tracked and secured.

DRS should study how other states and federal entities such as the Social Security Administration and the Internal Revenue Service test new computer systems, and then reduce as much as possible use of taxpayer "test subjects" in designing and testing new computer systems.

DRS should notify affected taxpayers and law enforcement agencies if a DRS employee improperly accesses taxpayers' information so judgments can be made whether a criminal investigation or other action is warranted.

Perhaps most troubling was that, prior to the implementation of additional security measures following this event, any DRS employee who had any level of computer network access could obtain through use of his or her computer any electronic file containing taxpayer information, meaning, quite simply, the information of over two million taxpayers, and that there was no

logging of who accessed what files (Auditors of Public Accounts, Office of the Attorney General, 2009). Eventually, following this event, James Norton, Chief of the Internal Audit, Planning and Development Division of the DRS, implemented security measures to address these issues.

CONCLUSION

The objective of this paper was to illustrate the practices of businesses and governments in collecting, analyzing and using Business Intelligence information, and discuss the ethical and privacy-related issues pertaining to these. Individuals usually determine the trustworthiness of a business or a government based on how the institution follows its own set of ethics. Furthermore, when the business ethics coincides with the individual's personal ethics a level of trust can be built. An individual may distrust the institution from handling the individual's information when the institution violates both institutional and personal ethics. In addition this may cause the individual to choose to not associate themselves with the institution. In a business sense this means, loss of business from that individual as well as a loss of information that individual would provide to help strengthen the business. For governmental institutions, this loss of trust could lead to restructuring or removal of government officials through voting or appointment from elected officials.

In some cases both businesses and governments make the determination that their own violations of ethics are done to prevent perceived future ethical violations. Laws have been created to close loopholes that both businesses and governments use to validate their decisions to break ethics of individuals. Unfortunately some laws lead to unforeseen consequences, such as enable, or force businesses and governments to break ethics of individuals.

The common thread of this has been individual ethics vs. institutional ethics and individual ethics vs. legal rights to information. It does come down to the decision of the individual and determining how much information you should be forced to provide and how much information that you do provide will be secured from public use. It is clear that as the individual's use of the Internet grows, and computer networks become ubiquitous, the challenges to an individual's privacy increases. However, the information collected by businesses and government are at times beneficial to the individual. However, faced with an information overload, the individual is often unable to determine extent of exposure of his/her private information, as also the exact extent of privacy protection he or she is entitled to. Given this, it is imperative that more laws be created that mandates that this information be provided in an easy, standardized manner to all Internet users. Further laws should also mandate punitive measure against any business or governmental agency that violates such measures to protect an individual's privacy.

REFERENCES

2011 Financial Tables. (2012). *Google.com*. Retrieved from http://investor.google.com/financial/tables.html

An Act Requiring the Establishment of a Searchable Database for State Expenditures, CT H. R. 5163. (2010). Retrieved from http://www.cga.ct.gov/2010/ACT/PA/ 2010PA-00155-R00HB-05163-PA.htm

Angwin, J., & Valentino-Devries, J. (2012, February 17). Google's iPhone tracking. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html

Applications results. (2012). *Ghostery.com*. Retrieved from http://www.ghostery.com

Associated Press. (1999, April 6). *Yahoo forums in privacy dispute*. Retrieved from http://www.nytimes.com/library/tech/99/04/biztech/articles/06yahoo-privacy.html

Auditors of Public Accounts, Office of the Attorney General. (2009). *Investigation pursuant to Conn. Gen. Stat. S.4-61dd concerning alleged mishandling of taxpayers' Social Security numbers at the Department of Revenue Services.*

Auditors of Public Accounts. (2011). *Special Review of the Transparency Database.*

Basulto, D. (2012, February 22). *Google, Safari and our final privacy wake-up call*. Retrieved from *The Washington Post.* Retrieved from http://www.washingtonpost.com/blogs/innovations/post/google-safari-and-our-final-privacy-wake-up-call/2010/12/20/gIQAS5N8SR_blog.html

Code of Conduct. (2009). *Google.com.* Retrieved from: http://investor.google.com/corporate/code-of-conduct.html

Electronic Frontier Foundation. (n.d.). *Privacy*. Retrieved from https://www.eff.org/issues/privacy

Federal Trade Commision. (1998). *Internet site agrees to settle FTC charges of deceptively collecting personal information in agency's first internet privacy case*. Retrieved from http://www.ftc.gov/opa/1998/08/geocitie.shtm

Federal Trade Commission. (2011). *Facebook dettles FTC charges that it deceived consumers by failing to keep privacy promises*. Retrieved from http://www.ftc.gov/opa/2011/11/privacysettlement.shtm

Frankel, M. (1998). Freedom of information act. *International Review of Law, Computers & Technology*, 121-146. doi: 10.1080/13600869855595

Hall, N. (2003, March 14). Sentence upheld. *The Vancouver Sun*, p. B7

Halzack, S. (2012, February 17). *FAQ: What privacy settings was Google flouting and why does it matter?* Retrieved from http://www.washingtonpost.com/business/economy/faq-what-privacy-settings-was-google-flouting-and-why-does-it-matter/2012/02/17/gIQADTE5JR_story.html

Hatch, D. (2012, March 11). The internet privacy paradox. *The National Journal* Retrieved from http://www.high beam.com/doc/1P3-2297192511.html

Hentoff, N. (2012, February 8). Government will know much more about you constantly. *Jewish World Review*. Retrieved from http://www.jewishworldreview.com/cols/hentoff020812.php3

Humphreys, A. (2012, February 18). They've got you on file: The growth of the database nation presents a grave danger to democracy. *National Post*, p. A10.

Internet Advertising Bureau. (2011). *Q3 '11 internet advertising revenues up 22% from year ago, climb to nearly $7.9 billion, according to IAB and PwC*. Retrieved from http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-113011

Introducing new DFA reporting. (2010). *Google.com.* Retrieved from http://www.google.com/doubleclick/

Miniwatts Marketing Group. (2012). *Internet usage statistics: The internet big picture: World internet users and polulation stats.* Retrieved from Internetworldstats.com: http://www.internetworldstats.com/stats.htm

Montana, J. (1998). The freedom of information act. *ARMA Records Management Quarterly, 32*(2), 46-51.

National Conference of State Legislatures. (2012). *State laws related to internet privacy*. Retrieved from http://www.ncsl.org/issues-research/telecom/state-laws-related-to-internet-privacy.aspx

Netmarketshare. (2012). *Browser market share*. Retrieved from http://marketshare.hitslink.com/report.aspx?qprid=0

Network Advertising Initiative. (2010). *Helping you protect your privacy online.* Retrieved from http://www.networkadvertising.org/index.asp

Ohio Legislative Service Commission. (2009). *Senate bills: Status report of legislation*. Retrieved from http://lsc.state.oh.us/coderev/sen127.nsf/Senate+Bill+Number/0248?OpenDocument

Privacy policy. (2008). *Amazon.com*. Retrieved from http://www.amazon.com/gp/help/customer/display.html?nodeId=468496

Privacy policy. (2012) *Google.com*. Retrieved from https://www.google.com/intl/en/policies/privacy/

Provance, J. (2008, December 3). GOP would restrict, punish data snooping. *The Toledo Blade*, p. A1. Retrieved from http://www.toledoblade.com/State/2008/12/03/GOP-would-restrict-punish-data-snooping.html

Real-life sharing. (2012). *Google.com*. Retrieved from.com: https://www.google.com/intl/en-US/+/learnmore/index.html#circles

Singleton, S. (2000, July 7). *How cookie-gate crumbles*. Retrieved from http://www.cato.org/publications/commentary/how-cookiegate-crumbles

Subramanian, R., & White, B. (2012). Teaching IS to the information society using an "informing science" perspective. *Informing Science: The International Journal of an Emerging Transdiscipline, 15*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2049422

The White House, Office of the Press Secretary. (2012). *Fact sheet: Plan to protect privacy in the internet age by adopting a consumer privacy bill of rights*. Retrieved from http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

United States Department of State. (2011). *Freedom of information act.* Retrieved from http://www.state.gov/documents/organization/183137.pdf

United States Government Accountability Office. (2008a). GAO: Privacy laws need revamping. *Health Data Management, 21*.

United States Government Accountability Office. (2008b). *Privacy: Alternatives exist for enhancing protection of personally identifiable information.* (Publication No. GAO-08-536). Retrieved from http://www.gao.gov/new.items/d08536.pdf

United States, Executive Office of the Prdesident, Office of Management and Budget. (2002). *E-government strategy: Simplified delivery of services to citizens.* Retrieved from http://www.usa.gov/Topics/Includes/Reference/egov_strategy.pdf

Vertical Web Media. (2012). *E-retail spending to increase 62% by 2016*. Retrieved from http://www.internetretailer.com/2012/02/27/e-retail-spending-increase-45-2016

This Page Was Left Blank Intentionally.