BTM 200 Lesson 1
Morals & Ethics

Privacy concerns in the digital world

Considering the full spectrum of privacy, people need to ask themselves if they are comfortable with all their characteristics in the public domain

The line, "if you've got nothing to hide, you have nothing to worry about" is used all too often in defending surveillance overreach.

While the argument applies to some problems, it represents a very narrow way of looking at privacy, especially given the array of privacy problems mixed up in government data collection and use beyond surveillance and disclosure. The "nothing to hide" argument, ultimately, has nothing to say.
A European paper issued by Michael Friedewald distinguishes seven types of privacy:

Privacy of the person
encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private;

Privacy of behaviour and action
includes sensitive issues such as sexual preferences and habits, political activities and religious practices;
Privacy of communication aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to email messages;

Privacy of data and image includes concerns about making sure that individuals' data is not automatically available to other individuals and organisations and that people can "exercise a substantial degree of control over that data and its use";

Privacy of thoughts and feelings refers to the right not to share their thoughts or feelings or to have those thoughts or feelings revealed. Individuals should have the right to think whatever they like;

Privacy of location and space means individuals have the right to move about in public or semi-public space without being identified, tracked or monitored;

Privacy of association (including group privacy) is concerned with people's right to associate with whomever they wish, without being monitored.
Considering the full spectrum of privacy, people must ask themselves: Are you sure you are comfortable with all of your characteristics in the public domain?
For example, do you want people to know where you spend your time - and who you like to spend it with? If you called a substance abuse counsellor, a suicide hotline or a divorce lawyer? What websites you read daily? The religious and political groups to which you belong?

Key privacy questions
Furthermore, as big data grows, enterprises need a robust data privacy solution to help prevent breaches and enforce security in a complex IT environment. In an Isaca whitepaper entitled *Privacy and Big Data*, we identify key questions that enterprises must ask and answer, which – if ignored – expose the enterprise to greater risk and damage. Here are five of them:

1. Can we trust our sources of big data?
2. What information are we collecting without exposing the enterprise to legal and regulatory battles?
3. How will we protect our sources, our processes and our decisions from theft and corruption?

4. What policies are in place to ensure that employees keep stakeholder information confidential during and after employment?
5. What actions are we taking that create trends that can be exploited by our rivals?

The problem is, the internet is a worldwide network and everything must be developed for a global environment without national borders. Many users approve a privacy policy without reading it, and many of these policies are vague guidelines where it is completely impossible for users to foresee the scope and content of their consent to the processing of their data. The consent to this agreement is mandatory to access the service. Consequently, users have no choice if they want to use it.

Shifting privacy standards

Furthermore, the service provider may change this policy. Everybody remembers the Instagram case. In December 2012, Instagram said it had the perpetual right to sell users' photographs for advertising purposes without payment or notification. Due to the strong reaction, Instagram backed down.

This brings to the forefront the fact that many consumers are poorly educated about how their personal data is collected by companies and are unsure about what it is actually used for. Investigation into the recent implementation of the EU Cookie Law has highlighted how misinformed consumers in Europe are.

In an April 2013 polling by Deloitte, UK web users polled said they had never heard of the EU cookie law. Only 15% of respondents said they knew at least a fair amount about it. This is surprising, given that an initial warning banner appears on UK websites informing the user if the site uses cookies.

In response to cookie banners, 56% of users said they either accepted or agreed to the site using cookies, or ignored the notices and simply carried on. Another 17% said they typically did not give permission for cookies, even if it meant not using the site. This corresponds closely to the percentage of those who said they generally browsed the internet with cookies disabled.

Google Glass

All of this is soon to be compounded by wearable technology, such as Google Glass, which is essentially a phone in front of your eyes with a front-facing camera. A heads-up display with facial recognition and eye-tracking technology can show icons or stats hovering above people you recognise, give directions as you walk and take video from your point of view.

In July 2013, Google published a new, more extensive FAQ on Google Glass. There are nine questions and answers listed under a section named Glass Security & Privacy, with several concentrating on the camera and video functionality.

But, crucially, this does not solve other privacy concerns.

Google Glass tracks your eye movements and makes data requests based on where you are looking. This means the device collects information without active permission. Eye movements are largely unconscious and have significant psychological meanings. For example, eye movements show who you are attracted to and how you weigh your purchase options when shopping.

How many of you will turn off your Glass while punching in your PIN? How about when a person's credit card is visible from the edge of your vision? How about when opening your bills, filing out tax information or filing out a health form? Remember that computers can recognise numbers and letters blazingly fast – even a passing glance as you walk past a stranger's wallet can mean that the device on your face learns his/her credit card number. All of this information can be compromised with a security breach, revealing both the information of the one using Google Glass and the people they surround themselves with.

On 4 July 2013, Chris Barrett, a documentary filmmaker, was wearing Google Glass for a fireworks show in Wildwood, New Jersey, when he happened upon a boardwalk brawl and subsequent arrest. The fact that the glasses were relatively unnoticeable made a big difference: "I think if I had a bigger camera there, the kid would

probably have punched me," Barrett said. The hands-free aspect of using Google Glass to record a scene made a big difference.

Privacy: Intrinsic right or social construct?
Privacy is entering a time of flux and social norms and legal systems are trying to catch up with the changes that digital technology has brought about. Privacy is a complex construct, influenced by many factors, and it can be difficult to future-proof business plans so they keep up with evolving technological developments and consumer expectations about the topic.
One way to ensure there are no surprises around privacy is by seeing it not as a right, but rather as an exchange between people and organisations, bound by the same principles of trust that facilitate effective social and business relationships.
This is an alternative to the approach of "privacy as right" that instead positions privacy as a social construct to be explicitly negotiated so it is appropriate to the social context in which the exchange takes place.

Isaca notes that enterprises eager to reap the benefits of big data and its vast potential must also recognise their responsibility to protect the privacy of the personal data gathered and analysed with big data. Risk management and maintaining adequate mechanisms to govern and protect privacy need to be major areas of focus in any big data initiative.
The lengthy privacy policies, thick with legalese that most services use now, will never go away, but better controls will, and should, emerge. Whatever tools are used to protect and collect personal data in the future, it will be important for companies such as Facebook and Google to educate their consumers and to provide them with options for all levels of privacy.

Cloud computing has emerged as one of the hottest topics in computer and information technology services. However, when data and services move to the cloud, there are a number of legal issues, including intellectual property issues, for both cloud computing providers and users to consider. These are complex issues, and a detailed discussion is beyond the scope of this article. Rather, this article is intended to highlight some of the issues and questions relating to intellectual property rights raised by cloud computing.

Background. The term "cloud computing" has several definitions. Cloud computing has been described as the delivery of computing as a service rather than a product, typically over the internet. In other words, data is stored and/or processed in the "cloud," which is a broad term generally used to describe infrastructure that is accessed remotely (i.e. the internet). Examples of cloud computing service models include: Software-as-a-Service (SaaS); Platform-as-a-Service (PaaS); or Infrastructure-as-a-Service (IaaS). Generally, SaaS models allow users to access and use software applications over the internet, rather than storing and running the applications locally. PaaS models provide access to a computing platform (such as Microsoft Windows, for example) on which applications may be run or developed. IaaS models provide access to computer infrastructure on which a computer platform may be run and maintained by the user. One of the potential advantages of cloud computing is that individuals or businesses may avoid the costs of buying, installing and maintaining hardware and/or software. The actual implementation of cloud computing systems and services varies greatly between systems.

As implied by the term "cloud," one aspect of cloud computing is the lack of a clear locality of hardware and data. Services may be sold to a client in a particular jurisdiction, and that client's data may be stored and processed at one or more locations in the same or other jurisdictions. The client may not have any knowledge of where the data is stored or processed. Data may be stored redundantly in multiple locations and in multiple jurisdictions, and may be split up and fragmented in storage. For example, data may be stored in different countries at different times making it difficult to determine where data is stored at a given time. Various parts or steps of data processing may also occur in different jurisdictions.

The vague and ambiguous nature of the "cloud" makes determining how the law will apply, or even what law will apply, a challenge. Because intellectual property rights are territorial, it is unclear in many instances what intellectual property laws will apply in the cloud computing environment.

Patent infringement. A Canadian patent grants the patentee the exclusive right to make, use and sell an invention for the term of the patent. A Canadian patent does not grant any rights in any other country. However, as noted above, cloud computing systems may extend across international borders. The multi-jurisdictional nature of cloud computing, and the uncertain nature of the "cloud," give rise to a number of possible complications for patent owners or licensees trying to assert their patents against potential infringers.

First, it may be difficult to predict what activities definitively constitute infringement. If a particular technology is patented in Canada, but a competitor's cloud computing service uses infrastructure and/or performs some or all of its data processing outside of Canada, the Canadian patent(s) may not be infringed. At the same time, a party wishing to avoid infringement simply by locating a component of a system covered by a competitor's patent, or by performing a step of a process covered by a competitor's patent, in a different country, may not succeed in avoiding infringement. For example, if a system is patented in the United States, infringement of the U.S. patent(s) by another party may occur even if a part of that party's system is located elsewhere (in Canada, for example). The law in Canada, however, is not clear on this point. Also, because the "cloud" may include components in multiple countries, the law in other countries may also need to be considered.

Second, cloud computing systems may include multiple components, each operated by a different party. For example, servers storing data may be owned and operated by one company, while system components relaying or processing data retrieved from those servers may be owned and operated by another company. These components may be contracted out to yet another company or companies, who then use(s) those components to provide services to users. Because different parties are responsible for providing different aspects of the system in this scenario, it may be that no single party infringes all of the elements of a patented invention. Instead, the practice of the elements of the invention may be divided between two or more parties. The Canadian *Patent Act* does not provide for divided infringement, and the issue has not been considered by the courts in Canada.

Third, even if the hardware or processes used in a cloud computing system do infringe patent rights, detecting the infringement may be difficult. As noted above, a user of a cloud computing service may not have any indication of where data storage and processing occurs. Thus, reverse engineering at the user's end to detect infringement may not be possible. A service provider's infrastructure may not be publically accessible in a manner that allows for efficient detection of patent infringement.

In view of the foregoing, one may consider whether any client-side elements of a cloud computing system are eligible for patent protection or for protection under other intellectual property regimes, such as copyright, for example. Activities at the client-side may be more localized and readily detectible. However, when obtaining protection for client-side elements of a cloud computing system, one should keep in mind who the potential infringer will be. It may not be in a company's best interest to assert patents against the users of a cloud computing service, since that may alienate those users from ever becoming customers. However, if the proper elements can be proved, a service provider may be liable for inducing the users to infringe.

Copyright infringement. As noted above, cloud computing involves the storage of data in the cloud rather than locally. This raises additional, potentially complex intellectual property issues. For example, the nebulous nature of cloud storage may complicate a copyright infringement analysis.

Copyright laws vary from jurisdiction to jurisdiction. What constitutes copyright infringement in one country may not in another. Therefore, when data is stored in multiple locations, it may be less clear whether copyright has been infringed in a particular jurisdiction than in situations where the location of a work is easily identifiable.

Another issue relating to copyright is whether cloud storage service providers can be held liable for copyright infringement. Canadian jurisprudence has held that an internet service provider acting as an intermediary for communication, and not itself engaging in acts that relate to the content of the communication (i.e. providing "a conduit" for information communicated by others), is shielded from liability by a provision of the Canadian *Copyright Act*. However, the question of whether cloud storage providers necessarily fit this definition of merely being an "intermediary" providing a "conduit" for information remains open. Therefore, the extent to which cloud storage providers may be shielded from liability for infringement under Canadian copyright law, based on the data stored for their users, is currently unclear.

Confidential information – trade secrets. Another concern relating to cloud storage is the protection of private and confidential data, such as trade secrets. Before uploading confidential data to the cloud, a user should consider what type of duty of confidentiality is owed to the user by the cloud storage service provider. Does that duty of confidentiality extend to sub-contractors utilized by the service provider? A potential user of a cloud storage service should also consider what will happen to data in the event that the cloud storage service is terminated.

Conclusion. Specific recommendations and outcomes related to complex cloud computing legal issues will be fact-specific. In many cases it is unclear how the law will be applied, because the issues have yet to be considered by the courts. Nevertheless, cloud computing providers and users alike should at least be aware of the issues identified above when considering how to best protect their intellectual property and how to avoid potential infringement pitfalls.

Computer Abuse Defined

Computer abuse is the use of a computer to do something improper or illegal. Examples of computer abuse include using a computer to expose personally identifiable information (PII) such as Social Security numbers, using a computer to change the content of a website owned by someone else, intentionally infecting one computer with a worm that will spread to other computers, using a computer to illegally share copyrighted items, and using one computer to gain unauthorized access to another. Other examples of computer abuse include cyberbullying and using a work computer for personal tasks on company time.

People who commit computer abuse may be violating university policies, company policies, or federal law. Responding to computer abuse involves identifying the offending computer(s) and then trying to identify the individual abuser(s).

Breaking Down Computer Abuse

Some definitions of computer abuse consider computer crime to be a type of computer abuse. Other definitions consider the two to be completely distinct, calling computer abuse something dishonest or unethical and computer crime something illegal. These opinions are irrelevant; however, when it comes to the federal law governing computer abuse: The Computer Fraud and Abuse Act of 1984 (CFAA).

The Computer Fraud and Abuse Act of 1984

The CFAA criminalizes certain types of computer abuse by banning “unauthorized access” of computers and networks. The law has been used to successfully prosecute both high- and low-level hackers for both civil and criminal matters. Early on, for example, the law was used to convict the man who released the first computer worm in 1988. Over the years, however, the law’s vagueness has resulted in punishments as severe as decades in prison for minor abuses that did not cause economic or physical harm.

While the law was intended for the prosecution of hackers committing computer abuse by stealing valuable information or causing damage when they break into a computer system. Congress has expanded the CFAA five times so that activities that were once misdemeanors are now federal felonies, and everyday users can be punished for minor infractions of an application’s terms of service.

The act makes white lies, such as understating your age or weight on a dating site a crime. It also makes violating a company's policy on using a work computer for personal use a felony. If the law were widely enforced, almost every white collar worker in America would be in prison for computer abuse. Because it is arbitrarily and sometimes overly enforced, federal judges and scholars have advocated for changing the law to decriminalize terms of service violations. One impediment to loosening the law has been resistance by corporations who benefit from it. One of the changes to the CFAA in 1994 amended the law to allow for civil actions, giving corporations a way to sue employees who steal company secrets.

Examples of Computer Abuse

An incident that many people might not think of as computer abuse is creating a fake social mediaaccount. If the social media service's terms and conditions require users to provide accurate information about their identities when creating an account, they could be prosecuted under the CFAA. This outcome is unlikely unless an individual uses a fake account for malicious purposes, such as cyberbullying, but it is a possibility—and that possibility of being prosecuted for something as minor as the mere creation of a fake account is a major problem with the CFAA. Attorneys have been able to exploit the law's weaknesses to defend clients who should perhaps have been punished, and prosecutors have been able to exploit the law to obtain convictions for minor incidents.

The most well-known example of the unintended consequences of expanding the Computer Fraud and Abuse Act was the threat of a 35-year prison sentence for internet activist Aaron Swartz for allegedly downloading millions of academic articles to which access was restricted through a subscription service, probably with the intent to freely distribute them. Arguably, Swartz's alleged actions would be constituted as theft, but did the proposed punishment fit the alleged crime? Swartz did not seem to think so—he took his own life before the case could go to trial.

Morals → conforming to established ideas of right and wrong.

Laws → formal standards that apply to all

- They are enforced by official agencies such as governments.
- Laws to cover all possibilities is impossible.
- Ethics

Ethical systems

a) Relativism

- No universal moral truth
- Moral principles governed by cultural tastes & customs
- Ex: women being shirtless at a beach.

b) Divine command

- God is all knowing, he sets morals and ethical standards.
- Gods law is right all should conform to it
- Breakings gods law is wrong.
- Ex: the ten commandments.

c) Utilitarianism

- Actions are judged solely by consequences. The outcomes of your actions should be judged.
- Actions that lead to, or produce happiness are considered superior to those that generate unhappiness.
- The greater good is more important than individual happiness.

d) Virtue

- Morals are found internally within a person
- Every individual should aim to behave well

- Ex: volunteers versus court-ordered community service.

e) Duty based (Deontology)
- Understanding and adopting a lifestyle in line with moral duties and rights.
- Everyone is expected to follow these moral duties and rights.

Unethical does not mean illegal. Illegal does not mean unethical.

- Amoral behavior means no sense of right or wrong and the lack of awareness or interest in the consequences.

Sources of Personal Ethics
- Religion
- Family
- Experience
- Teachers
- Friends
- Reflection

Ethics & Society

• Social rules of conduct exist.
• Ignoring them can have an impact.
• Considering them may provide health benefits. • Rejecting them may produce stress.
• See Positive Psychology
• Causes of happiness
• Identifying personal strengths and values
• Negative [cheating, stealing, selfishness, lying] versus positive [generosity, honesty, trust]

Technology Challenges

• Technology advances continue to challenge the boundaries for ethics and moral behavior.
• Examples:
• Social justice: Programming ethics into robots. Who should do it? Who should govern it?

- Intellectual property: 3D printing misuse. Can regulations be imposed?
- Privacy: Human implanted data chips. Societal benefit or privacy violation?
- Property rights: Who owns outer space?
- Computer abuse: Is organized hacking a mode of terrorism.