Available online at eruditio.worldacademy.org
Eruditio
e-Journal of the World Academy of Art & Science
Volume 1 Issue 4 - March-April 2014

Privacy is Not Dead, it is Just Resting

Graeme Maxton
Member, Club of Rome

"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." – ***Benjamin Franklin***

Abstract

Our right to privacy is under assault. Companies are collecting more information about how we live and our views, often with questionable motives. At the same time, many governments are tracking their citizens more than ever before.

Privacy is not just about keeping a bank account hidden or a love affair a secret. It is about freedom. It is about the right to do what we want to do and express our thoughts, alone or with others, without being watched. It is an essential component of relationships, offering intimacy and allowing shared discussions and experiences. It is what has separated modern societies from totalitarian regimes. If what we do and where we go are tracked and recorded, we tend to change our behaviour. If what we write or say is monitored, we hold back.

Despite its importance, new technologies and laws have allowed the privacy of millions of people to be invaded. A fundamental right is evaporating. If we let the trend continue, we risk losing almost everything enlightened modern societies hold dear.

1. Don't Shout Across the Room at Parties

When Mark Zuckerberg, the founder of Facebook, said in 2010 that he thought that people wanted to be more open about sharing personal information he was suggesting that our views on personal privacy have shifted greatly in a very short time. When he and others founded Facebook just six years earlier, he said, "the question a lot of people asked was 'why would I want to put any information on the Internet at all?'"

Today, the generation of Facebook fans and LinkedIn lovers no longer cares about the information they post. Hundreds of millions share intimate details of their lives. They shrug when Facebook and its rivals change their privacy policies to make this information more widely available, deeming their privacy irrelevant or unimportant. As Zuckerberg says, information about us has become public by default.

Yet there remains the question about who or what is driving the change and why. Is the new openness about personal information the result of fundamental changes that have taken place in our societies? Do people no longer care about their privacy? Or is the change being driven by companies wanting to profit from prying into our lives? Can we trust Facebook, Yahoo, MySpace, Bing, Google, Skype, Microsoft, Apple and others with the information we have given them and that which they have collected themselves?

That would certainly seem rash, especially after recent revelations over their close links to America's national security apparatus. The fact that these firms are so large and powerful is itself reason to worry. Because they have almost no competition, dominant companies have a tendency to exploit customers and markets, as the oil, rail-road and banking barons of the 19th century did. Today's big American technology companies don't control the electricity supplies, bank lending or transport routes, however. They control something much more powerful – information.

Using the information they hold, these firms now have the ability to track individuals and groups with similar views and ideas, whether they are in contact or not. They know who is left-leaning, who is gay, who is worried about their weight. They know who our friends are and where they are, even when we do not. They have the ability to nudge our views in directions they might find beneficial – to make us think more favourably about particular products or negatively about issues like privacy, for example. Through the use of 'sock-puppets', fake online personae used by marketing firms and government organisations, they can manipulate our opinions about news events and politics.

Recent technological developments raise other concerns. The latest generation of tablets and smartphones are able to report their location, even when they are switched off. Software makers and telephone companies can keep track of where we are and where we have been. The next generation of phones will even be able to track the type of movement being undertaken – a car journey, a walk, a train ride, for example.

More troubling still, the activities of the big technology companies, and what they do with the information they hold are almost completely unregulated. Within the US, the authorities have said that regulations would hinder commercial interests and so companies such as Facebook and Google will only face a biannual audit of their activities for the next 20 years. New regulations are being developed in Europe, India and China but they will not come into force for several years. For others, indeed for the majority of users, what these companies collect and what they do with the data are beyond the scope of national laws. This is especially troubling because these big firms have already shown very poor ethical standards.

2. Two-Facedbook and Twittish Twitter

Intel, Google and Microsoft have all been fined for anticompetitive behaviour. Apple and Skype have been repeatedly investigated and accused of it. Google was caught getting around the privacy settings on its own browser by placing tracking cookies[1] on websites. The US Federal Trade Commission (FTC) says Facebook has 'repeatedly' failed to honour its promises to keep personal information private,[2] has continued to make information available even after users deactivated or deleted accounts, and shared information with advertisers and developers when it had promised not to. Google collected information about internet access points and user details illegally with its Streetview car and then failed to delete the data despite repeated assurances that it would.[3] Many of Apple's programs have been found to be 'harvesting user information, including entire address books' without the users' permission.[4] Twitter has acknowledged that it has stored customers' address lists on its servers too, without them knowing. When this was discovered, instead of apologising, the company amended its privacy policy to make the practice standard.

Sergey Brin, one of Google's founders, famously once said that the perfect search engine would be 'like the mind of God'. It would be everywhere and know everything. By combining the information it collects from all the sites it operates, the company appears to be making every effort to develop this, a system that knows you better than you probably know yourself.

Google's main search engine tracks your interests and then filters the results you see, depending on your previous searches. It tracks the sites you visit. YouTube, which Google owns, tracks your taste in videos. Streetview Google Earth and Google Maps offer a picture of where you live and where you go. Picasa, Google's photo sharing website, uses facial recognition software to identify you and your friends. Gmail knows who you write to and what you say. Google Docs stores your letters, Google Calendar your plans. The company's Android operating system on your phone or tablet knows exactly where you are and where you have been. Changes to the company's privacy policy in 2012 allow it to collate all this information.

By integrating so much information, Google even has the ability to track those who are not active on its sites. As long as your friends are talking about you and posting your picture, you and your movements are being logged.

3. Not Now Google

Taking this a step further is a system called 'Google Now' which collects everything that Google knows about you and then tries to create a 'theory of you' to predict your needs. This is called 'push search'; rather than posing questions, the system tries to give you answers before you ask.

Google Now knows, for example, where you are likely to be at certain times of the day, ties this to information about where you actually are, and then tries to predict what you will do next. If you have an appointment in your Google Calendar, and usually travel by bus, it will tell you when you need to leave. If you have bought a flight ticket online, it will know this and so tell you about any air-traffic delays. If you are in the car, it will learn where you go or where you recently thought of going based on your searches. So it will make suggestions and tell you how long the journey should take, given the traffic conditions. The system also gives you updates on your favourite sports teams, which it works out from your searches.

Google Now is obviously good for advertisers, because it helps them target their messages better. Journalists report that the system is 'creepily self-aware'. Yet the question is: should Google be permitted to have a theory about any of us? Should a private company, one found guilty of collecting private data illegally, have so much information about us that it can help direct our lives? Rather than simply trying to predict what we do, the risk is that it will try to influence or determine the outcome. Rather than being helpful, it has the capacity to modify our experiences and ideas, either to the benefit of advertisers or for some social or political end.

4. The State is Watching You Too

Our privacy is not only under assault from big American technology companies. Governments are invading the privacy of citizens more than ever before, often illegally.

Millions of people are being watched, tagged and monitored by their governments, even though most are not guilty of any crime, will not be charged with any offence and, until Edward Snowden's revelations in the summer of 2013, did not even know they were being spied on. Even now, they are told that the snooping is essential to combat crime and fight terrorism.

The traditional approach to tackling crime is to wait for an offence to be committed and then use investigative techniques to catch the culprits. Its success depends partly on people being dissuaded from committing crimes, through education, instilling a sense of social responsibility and having penalties severe enough to put them off. It is the enlightened approach to crime and assumes, at its core, that good society is based on trust.

The new approach supplements the traditional model with technologies that can make investigations simpler, though these also carry costs. They make it possible for some serious crimes to be stopped before they are committed and so can save lives. They make solving some crimes easier. By using the location tracking system on mobile phones or CCTV cameras for example, the police can identify who was present when a crime was committed. By reading the emails sent between members of a suspected terrorist cell, the security services can keep an eye on what they are planning.

Inherent within this approach however, is an assumption that innocent people will not mind being watched too. For it to work, the security services need to monitor people they think might commit a crime. And sometimes they will get that wrong. They will also track people who abandon plans to commit a crime – who may do nothing illegal either. And they will inevitably track the friends of possible wrong-doers, to see if they are involved. The new approach means that many people are tracked, with their friendships and movements watched, logged and recorded without them knowing, when they are not guilty of anything.

To function, the modern approach requires every citizen to accept that they may be monitored. Everyone has to trade a possible loss of privacy for greater security. They have to accept that the details of their lives may be tracked and stored without their knowledge and for no good purpose. Moreover, they have to accept this imposition without their agreement, and under the assumption that the powers given to the police and security services to do this will not be abused.

Despite the obvious advantages, the drawbacks with this approach are many and grave. It undermines the fundamental right to a presumption of innocence. By tracking us, there is an inherent doubt, a small assumption that we may be guilty of something. The system is also easy to abuse and it's hard to track when it is. It can lead to a state that is effectively controlled by the police, where people are fearful about what they do, say and think.

Despite these disadvantages, such modern crime-fighting thinking lay behind the creation of America's Information Awareness Office (IAO) in 2002. This was established to build a database on everyone. Its goal was to create Total Information Awareness (TIA), a computer program that would collect data about all of us and then interrogate this to identify patterns of interest. Without having to apply for a search warrant, the IAO wanted to collate information from personal emails, financial transactions, medical records and social networks and so build a picture of every individual in America and ultimately everywhere else too. This was

to be used to identify suspicious activity, unhealthy relationships and threats. The original IAO program included funding to collect biometric data too, and allow people to be tracked using a network of surveillance cameras.

Less than two years after it started, the IAO was shut down by Congress because of fears that it would lead to a mass surveillance system. Yet its ideas are still with us and many of its projects have been given the funding they needed. What it set out to achieve has been created, in other ways and under a different name. The master software program has been renamed 'Stellar Wind' or simply 'The Program' and, despite legal objections on constitutional grounds from top Justice Department Officials,[5] the massive computer needed to interrogate all the information is nearly complete.

The NSA's $2 billion data storage facility will eventually have the capacity to process yottabytes (a quadrillion gigabytes or 10 to the power of 24 bytes or 500 quitillion pages of text) of data and, from 2014, it will be the centre-piece of a 'Global Information Grid',[6] with the capacity to store personal information for decades.

The blandly-named Utah Data Center will intercept, decipher, analyse and store vast swaths of the world's communications. With the help of an array of listening posts and satellites, it will capture and store the contents of private emails, phone calls, and Google searches, as well as all sorts of other personal data trails – parking receipts, travel itineraries and store purchases. Because of its vast computing power and the huge number of messages that can be analysed simultaneously, which make it easier to identify patterns, the Centre will also be capable of deciphering previously encrypted material. This will give America access to an even wider range of password-protected data than now, including financial information, commercial reports, databases, stock transactions, business deals, foreign military and diplomatic secrets, legal documents and other private personal communications.

Rather than being pulled together by the government as was envisaged under the establishment of the IAO, the data needed to feed this computer will come from private companies. Google, Facebook, Twitter, Apple and all the others have collected all the information needed, and even more effectively than originally envisaged. Congress has not been able to object.

By tapping into Facebook and other social networking sites, the authorities in America and much of Europe know who our friends are, what we do and what we like. Google's data tell them our interests. Mobile phone apps show them where we are, to within a few feet. Twitter is used to identify 'communication clusters',[7] groups of people with similar views and the opinion leaders they gather around. Twitter was especially useful in pinpointing the ring-leaders during the Occupy movement's sit-ins in late 2011 and has also been used to track Tea-Party thinking, to predict which political candidate members we will want to follow.

5. Sharing More Than You Intend

The creation of this giant computer and database is not the only developments that should bother us, however. Part of the IAO's original remit included mining the information hidden in metadata. This capability has also been developed.

Metadata is the technical name for the hidden content on our computers, the electronic DNA. Metadata lie behind all websites, videos and electronic documents. They show when

computer files were created, where they are located on a hard drive and when they were accessed or changed. They show the location and identification of the computer as well as the name of the user and the Internet Service Provider. They show the changes made to documents, revealing what the writer added and deleted. Comments made by those editing the text are also traceable. This is also true for those who use cloud computing services and for files converted into PDF format. (Metadata can be removed though.)

Metadata can be used to show, for example, that a series of pictures was taken using the same camera. If they were taken using a camera with a location detector, the metadata show the precise location of the picture. It can be proved that photos said to have been taken in New York were actually snapped in Hong Kong.

Lawyers and government agencies value metadata because they are so revealing. Metadata 'mining technologies' have been developed to identify the thinking behind documents and reveal the details of who contributed to them. US security agencies have developed meta-metadata analysis tools, which mine the metadata about the metadata. And, crucially, websites such as Google and Facebook, which promise to protect some of your information in their privacy policies, do not promise to protect users' metadata. They class them as business information which they retain and store indefinitely.

Scalable Social Network Analysis (SSNA) software was originally a creation of the IAO too. The IAO's plan was to create a program that would analyse real life social networks – families, sports teams, legislatures—for attributes that were interesting or valuable. Today, the software is used commercially to analyse data contained in email, sent on Twitter or posted on Facebook and Flickr to target advertising. It is also used commercially in the online gaming industry, and to track buyer behaviour.

For governments SSNA software is used to extract and review parts of speech and distil text. It looks at patterns and relationships hidden on social networking sites, in phone conversations and in corporate data. It is used to identify fraud, find hidden terror cells, track money launderers and seek out organised crime syndicates. It can be used to monitor people's personal interests too, track their friendships and affiliations and understand their wants, beliefs, written thoughts and activities.

6. No 'Reasonable Expectation of Privacy'

Such developments, while technically impressive, are also worrying. The government agencies that use them (and not just in America) freely admit that they are compromising privacy.[8] Thanks to changes in laws since 9/11 however, most of these methods of collecting data are legal – though not all.

Technologies of more questionable legality have also been developed and used by several government agencies, including computer viruses and Trojan software deliberately used to infiltrate computers. Examples include CIPAV* and Magic Lantern.†

Magic Lantern tracks keystrokes and is installed via an email attachment or by exploiting the vulnerabilities in computer systems. The FBI originally wanted to activate the program

* See https://en.wikipedia.org/wiki/Computer_and_Internet_Protocol_Address_Verifier

† See https://en.wikipedia.org/wiki/Magic_Lantern_(software)

when someone started to use PGP encryption to protect their email messages, to allow them to open sealed documents.

CIPAV is a virus tool used by the FBI to gather location data. It identifies the address of a computer, the open ports, installed applications, operating system and web browser while tracking the websites visited. Its existence was exposed in 2007 during the trial of a boy who made bomb threats to his school near Seattle.[9] His computer had been infected with the software through MySpace. Controversially, the US Circuit Court of Appeals ruled that the FBI's actions were legal as Internet users no longer have any 'reasonable expectation of privacy'.

The FBI has also developed an internet traffic 'packet sniffing' program called Carnivore. This is installed on the computers of Internet Service Providers and used to track messages in transit.

7. Micro-brother is Watching Too

Governments are not just using computers to track their citizens. According to *The Washington Post,*[10] technologies and techniques honed on the battlefields of Iraq and Afghanistan are in the hands of British and American law enforcement agencies now too, allowing mass surveillance of their citizens.[11]

In the UK, almost all towns and cities are already under 24-hour CCTV surveillance. Many cameras are fitted with facial recognition technology and microphones to listen into nearby conversations. British[12] and US authorities have also started to use unmanned aerial drones to monitor citizens and gather evidence for prosecutions. In the US, these aircraft can stay airborne for up to 15 hours, and watch from a height of up to 7,000 metres, using cameras, infra-red sensors and radar.

In England and Wales, the police have collected DNA from 6 million citizens* – more than one in eight adults, creating the largest database of its kind in the world. Samples are taken from anyone detained at a police station, even if they are not charged with a crime. Although the police wanted to retain these samples indefinitely, a ruling by the European Court of Human Rights means that samples of those convicted of non-serious crimes will only be kept for between six and twelve years. Others will be retained indefinitely.

Records of people's emails, telephone numbers dialled, online games playing, web-browsing and chat-room activities are also now stored in many Western countries for many years, by law. This includes information about text messages, Google searches and Facebook friends. Many authorities record all travel into and out of their country too, including details of itineraries, seat reservations, addresses, credit cards and phone numbers accessed.

Those wanting to avoid such intrusions will find it hard. Not being on the Internet and not having a smartphone does not mean you cannot be tracked. Your face has probably already been logged, apart from your being followed through other electronic activities such as credit card use. Thanks to automatically tagged photographs on social media sites, the FBI[13] is now tapping this as a new source of intelligence. With the latest security cameras able to search through 36 million faces in just one mouse-click, remaining anonymous is hard. Even

* As of the end of 2012

wearing a mask, dark glasses and a wig will not help. Thanks to another part of the IAO initiative, Human Identification at a Distance (HumanID) software makes it possible to identify your gait, the way you walk, from up to 150 metres.

8. Yesterday's Idea And Tomorrow's Too

With so much snooping, it is easy to imagine an Orwellian future, with televisions spying on their viewers, microwave ovens recording dinner conversations and beds reporting the dreams of those who sleep in them. At issue is not just how much of our lives is suddenly being recorded; it is also the pace of change that matters. Thanks to technological developments and new pieces of legislation, the level and sorts of monitoring have expanded astonishingly quickly in little more than a decade while laws designed to protect us have struggled to keep up.

"Basic freedom to behave as individuals is being compromised."

The reason most people are unperturbed by these developments is that the risks attached to them still remain unclear. Moreover, we are led to believe that the changes are both necessary and useful.

Although privacy is protected under Article 8 of the European Convention on Human Rights (ECHR),* additional rules will come into force by 2016 to provide new safeguards. Companies operating in the EU will need to gain consent, which will be strictly defined, before they can use or process data about European citizens. They will only be permitted to collect the information they need and they will only be able to keep it when they need it. Moreover, any data held must be movable, so that it can be taken down from a social network site whenever a user wishes. European citizens may also be given a new right – the right to be forgotten. They will be able to see the information a company holds on them and demand that all copies be deleted.

While such regulations will undoubtedly help, and they only help those in Europe, they treat the symptoms, not the problem.

The question they fail to tackle is, why are these companies and our governments invading our privacy at all? Humankind has survived for centuries without this sort of intrusion and there is scant evidence that it is making the world any safer. It may have made the job of policing a little simpler and allowed companies to sell a few more products. But the majority of people are worse off, because their basic freedom to behave as individuals is being compromised.

It is especially hard to justify this government intrusion when the risk of terrorism is so small. The number of deaths caused by terrorist attacks in the US and Europe since 9/11 is tiny compared to those caused by heart disease, road accidents and even child-birth. Yet Western governments have built a massive network of computers to spy on their citizens, while doing little to address problems that are real and urgent – such as climate change and youth unemployment.

* Contrary to popular opinion this Convention and the Court which hears related cases are not part of the European Union (EU). The treaty came into force several years before those needed to form the EU were developed. There is a link now though, with any new member of the EU required to sign the ECHR. Even so, there are more than 20 signatories who are not members of the EU, including Turkey which was a founding signatory, and Russia.

9. Without Change, We Will Behave Differently

Of course, the right to privacy has been breached throughout history. The difference between then and now though, is that what used to be an exception is now done automatically and few people question it. Worse, much of the surveillance is done in secret, with little or no oversight by courts or elected bodies.

"The invasions of privacy we have seen in the last ten years will gradually destroy our basic right to freedom unless they are stopped."

In *Delete – The Virtue of Forgetting in the Digital Age,* Viktor Mayer-Schönberger tells a story about a Vancouver-based psychotherapist, Andrew Feldmar.[14] In 2006, Feldmar tried to cross the Canada-US border – something he had done many times before. On this occasion though, the guard searched online and found that he had written in a medical journal about taking LSD in the 1960s and so he was barred from entry.

The following year, Stacy Snyder, a Pennsylvania teaching student, posted a picture of herself at a party on MySpace.[15] She was wearing a pirate's hat and holding a plastic cup which may have contained alcohol. Classmates saw the photo and reported her for breaking college rules. As a consequence, she was denied her leaving certificate, which effectively ended her teaching career.

Many more examples illustrate that the information being collected by private companies and governments has the capacity to change our lives in ways we can barely imagine. It has the potential to change what we do, write and say. What we do will be recorded, posted and stored. What we write will be read by people other than those intended. What we say will be taped and filed.

If we cannot delete or modify these data, the information being uploaded about us risks imprisoning us in our past, never allowing us to forget. It takes away a vital and natural part of what it means to be a social person, the ability to put the past behind us at times. Without change, embarrassing pictures, angry tweets and bitter blog postings will remain in the ether forever, and with them our embarrassment.

Not being able to escape the past will make us frightened of the future too. We will worry that information we post tomorrow might be used against us later. That will make us change how we behave. As more non-digital records are scanned and uploaded, even those things we did before the Internet era have the potential to haunt us again too.

If we do not stop these trends, they will force us to organise our societies and handle our relationships differently, making us become more secretive and frightened. They will infect our ability to make judgements and act spontaneously. They will affect our ability to live our lives as we choose.

The invasions of privacy we have seen in the last ten years will gradually destroy our basic right to freedom unless they are stopped.

Author Contact Information
Email: me@graememaxton.com

Notes

1. "Google circumvented privacy settings for Safari on iOS, Mac," *Macworld* http://www.macworld.com/article/165455/2012/02/google_circumvented_privacy_settings_for_safari_on_ios_mac.html
2. "Facebook's Eroding Privacy Policy: A Timeline," *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2010/04/facebook-timeline "Facebook addresses several privacy problems," American Civil Liberties Union Blog. http://www.aclu.org/blog/content/facebook-addresses-several-privacy-problems
3. Matt Warman, "Google failed to delete Streetview data," *Daily Telegraph,* 27th July 2012 http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/9433908/Google-failed-to-delete-Streetview-data.html
4. "Social apps 'harvest smartphone contacts'," *BBC,* 15th February 2012 http://www.bbc.com/news/technology-17051910
5. "The Program," *New York Times,* 22nd August 2012 http://www.nytimes.com/2012/08/23/opinion/the-national-security-agencys-domestic-spying-program.html?_r=1
6. "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired Magazine,* 15th March 2012 http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/4/
7. "Occupy vs Tea Party: what their Twitter networks reveal," *New Scientist,* 17th November 2011 http://www.newscientist.com/blogs/onepercent/2011/11/occupy-vs-tea-party-what-their.html
8. Jason Ethier, "Current Research in Social Networking Theory," *Northeastern University.* http://www.atkinson.yorku.ca/~sosc2410/Social%20Network%20Theory2.pdf
9. "FBI's secret software keeps track of teen who made bomb threats," *Wired Magazine,* 18th July 2007
10. "Monitoring America," *Washington Post* http://projects.washingtonpost.com/top-secret-america/articles/monitoring-america/
11. "International Privacy Ranking," *Privacy International* https://www.privacyinternational.org/reports/surveillance-monitor-2007-international-country-rankings
12. "Drone makes first UK 'arrest' as police catch car thief hiding under bushes," *Daily Mail,* 12th February 2010 http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html "Police drone crashes into River Mersey," *BBC*, 31st October 2011 http://www.bbc.co.uk/news/uk-england-merseyside-15520279
13. "FBI would like to follow you on Facebook and Twitter," *Russia Today,* 26th January 2012 http://www.rt.com/news/fbi-social-networks-privacy-781/
14. "LSD as Therapy? Write about It, Get Barred from US," *The Tyee,* 23rd April 2007 http://thetyee.ca/News/2007/04/23/Feldmar/
15. "How to Lose Your Job on Your Own Time," *New York Times,* 30th December 2007 http://www.nytimes.com/2007/12/30/business/30digi.html?_r=1