

Using Information Technology in Personal Profiling

Introduction

Information technology has affected a number of large societal changes in recent years, including that of privacy, or more specifically, personal profiling. First, it is important to establish why privacy is an important issue and how personal profiling relates to the issue of privacy. The importance of privacy is summarised quite nicely in [1], where two reasons are given. The first reason is that by choosing what information we disclose about ourselves, we maintain our individuality. The second, and more pertinent reason is that privacy allows us anonymity. Without anonymity, people would not be able to speak freely, without fear of persecution. Personal profiling violates both of these freedoms. It is important that uses of personal profiling and data retention are closely and tightly regulated, to avoid encroaching on civil rights. For example, a Florida man was recently awarded \$500,000 for to his unfair removal from a flight due to his wrongful association with a group of people due to his appearance[2]. There are few laws to protect people that are wrongly associated with a particular group or organisation.

Before the advent of desktop computing and cheap commodity computers, creating copies of data would often require someone to journey to a particular location, request files which would have to be manually retrieved, and to physically take down a copy of said data. The advent of information technology has meant that most personal data is kept electronically and the barrier to retrieving and copying this data is all but eliminated. Due to this, there is an increased responsibility for large organisations when dealing with personal information. It is a lucrative opportunity to sell personal information to third parties, but doing so can jeopardise people's privacies, and in more extreme cases, cause financial and physical harm (for example, such cases as where selling information leads to identity fraud). Many laws have been passed in the last decade to help recognise and resolve the traps and ambiguities in this area, and to protect peoples' privacies and human rights.

With these points made, it is also important to note that personal profiling affords us many benefits, along with the associated issues that must be considered and dealt with. Arguably, targeted advertising is a benefit. It is often more desirable to see adverts that are related to our personal interests, than those that are not relevant to us. Targeted advertising is enabled by technologies such as Google Mail's keyword-extraction, allowing a profile of our interests to be created live as we read our mail. Modern technology allows this to happen without sharing this information with any third parties and without any human participation[3]. Personal profiling can also benefit national security. By building a profile of a particular group of offenders, people matching this profile can be prioritised in terms of police attention. This is a hotly debated area, however, as profiling the wrong information can lead to a particular group of people being discriminated against. In this report, some of the advantages and disadvantages of information technology in personal profiling will be explored and discussed. Conclusions will be drawn from the researched information and my personal thoughts will be summarised at the end of the document.

Negative Uses and Pit-falls of Personal Profiling

Personal profiling can be very easily misused and so the privacy issues associated with it must be treated very seriously. The security issues that are associated with technology and personal profiling were probably first brought to the fore in the mid-70s. As large government and corporate databases were becoming more commonplace, abuses of digitally-stored personal information were also becoming more common. This brought about the U.S. Privacy Act of 1974[10], which states (in part) “*No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains*”. This act was later mirrored in the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)[11], which also formed the basis for the British Data Protection Act (1984)[12]. As an aside, the Data Protection Act was amended in July 1998 to conform to the requirements of the European Union's Data Protection Directive, of which changes included that entities that maintain records register with the Information Commissioner. This amendment would allow for closer regulation.

This brings about the issue of presumed versus informed consent, as discussed in [4]. When volunteering personal information, consent as to what is allowed to be done with this data is often presumed and it is up to the volunteer to 'opt-out'. This is of particular concern when dealing with on-line advertising. It is quite possible for the advertising networks to collect data about users' browsing habits without their consent. Under American law, there are some restrictions as to the information which an advertising agency is allowed to collect and the ways in which it can be collated, however, some information collection is allowed without users' consent[13]. The implications of this are that information may be collected without users' knowledge, and thus, without their permission. This has been a widely criticised policy, yet Britain has also followed suit with an opt-out policy on personal profiling. European parliament on the other hand has called for an opt-in approach, stating that users must be informed and required to give permission before a personal profile is created[14].

It is clear that the law is struggling to keep up with the advancements being made in IT, allowing people to share data more easily and freely. A particular concern is that although personal data is governed by the acts and regulations discussed previously, these same rules do not always apply to data that is derived from this originally volunteered information[4]. This allows for personal profiles to be derived from what appears to be fairly un-identifying information and it is not in the power of a subject to view, amend or remove this data. This can lead to cases, such as that mentioned in the introduction[2], where a particular person is wrongly identified as belonging to a group profile due to derived information. As small bits of personal data are collected about a person with their consent, information could be derived and shared from this; information which the subject would not have knowingly consented to being collected, and which may be inaccurate. Although only privacy in private has been discussed, privacy in public is also affected by these same issues[5]. For example, information that someone may willingly divulge in a public situation, such as their hobbies or feelings on social issues may not be information they'd want a prospective employer to have knowledge of. Public surveillance is also an issue, as information about shopping trends and preferences can easily be derived by recording a person's movements in public. These issues are related to the aggregation of personal information to create a personal profile. It is not always clear that giving consent to record apparently-harmless or worthless personal information can lead to less harmless information being derived or collated.

Positive Uses of Personal Profiling

With all the negative aspects associated with personal profiling and the issues surrounding it, it is easy to forget the positives that can result through its use. A number of interesting projects have been enabled primarily through the use of personal profiling. For example, the paper "*The Design of Personal Mobile Technologies for Lifelong Learning*"[7] talks about creating a framework for a wearable personal computer system that grows and evolves with its user to enable learning at any point throughout their lifetime. It is clear that such a technology could not be implemented without the ability to freely record personal information and make derivations from such. These learning devices would be able to communicate with each other, for example, sending a learner's work with a teacher. The paper also makes mention of a lifelong learning device as a "communications aid". Listed abilities include a web-site presenting different information depending on a users abilities or previous activities. Such a feature would not be possible without extensive personal profiling, and the ability to communicate and process these profiles with remote clients. Although there are several security issues associated with this idea, it is clear that such a device would help people realise opportunities and maximise on their potential more readily. Such work can also be seen in the One Laptop Per Child project (also referred to as the \$100 laptop project)[15].

Another positive application of personal profiling is that of electronic personal agents. Personal agents have the ability to gather and/or organise information for a user, based on their preferences and habits. A good personal agent works almost transparently to the user. To quote the paper "*Adaptive Personal Agents*"[8], "*Personal agents require a user model, or personal profile*", and "*For optimal use, personal agents must be able to learn a user's preferences and habits over time*". This paper goes on to say that features of a desirable agent also include the ability to share information and collaborate with each other. Clearly, an application that has free reign to gather information about personal habits and share that information with others is rife with security and ethics issues. This area is also covered in detail by this paper, where it describes it as the "*most crucial obstacle facing personal agents*". Users must be able to trust their agents, as they will be making suggestions to them, and possibly even making decisions on their behalf. It is quite possible for a company that provides agents to skew suggestions made in favour of them, or to withhold suggestions that may be detrimental to them. Due to this issue of trust, an unrestricted agent will probably never be realised outside of the academic or open-source community. Trust becomes less of an issue, however, when restrictions are imposed on their domain, as is also stated in the paper.

One final and less theoretical positive application is that of product suggestions in on-line shopping. This is a feature that almost anyone who has shopped at a major on-line retailer would have encountered, and possibly taken advantage of. Product suggestions could be viewed as a form of targeted advertising, and are often far less intrusive and offensive than untargeted advertising. Product suggestions are listed as one of the desirable features of both a physical and a virtual store in the paper "*Technology and the Customer Interface: What Consumers Want in the Physical and Virtual Store*"[9], a claim that is backed up with survey evidence. This goes to show that despite the generally negative public view on surveillance and profiling, that when employed in a way that will advantage the subject, personal profiling will be accepted and provide a more pleasant experience than without it.

Summary and Conclusion

The advance of information technology has enabled many new technologies, and caused our handling of many old technologies and methods to adapt. While we struggle as a society to keep up, with new laws and legislations, technology still progresses at a high rate, causing us to consider new issues and reconsider old ones. The major issue with personal profiling at the moment is that of privacy and trust. Personal profiling can be a powerful tool, but can also be easily abused, as evidenced by the amount of laws that are associated with it, and its prevalence in recent news. Uses of personal profiling range from agents, to advertising, to national security (an issue that goes relatively unmentioned in this report) and it will only become a bigger issue in the future.

While a mostly negative image of personal profiling has been portrayed in this report, it is important to note that it is a concept that will be very important in the advancement of many areas of society. Most importantly, these include education and business, where technologies that rely on personal profiling, such as agents, can massively increase efficiency and productivity. Fortunately, the importance of this issue seems to be clear to governing bodies (where Europe seems to be particularly progressive), and is being made increasingly public. It is becoming less easy for companies to discriminate based on incorrect or biased profiling, and this can only be considered a good thing.

My own opinion on personal profiling is that it's an overall positive concept. I enjoy the benefits of personal profiling when I browse the web, and wish to further take advantage of it, to ease day-to-day activities. I often take advantage of shopping and music recommendations, and I find that targeted adverts are less offensive than those that are completely unrelated to me. I am not unaware of the issues involved with personal profiling, however, and I worry that current legislation is not enough to prevent common misuses of personal information. I also worry that different legislature in different countries is confusing the issue for international business; something which is very common on the internet. I think that people will become more accepting of personal profiling as it is subtly integrated into day-to-day activities, rather than the extensive profiling that would be suddenly forced onto people when using agents.

References

- [1] <http://www.privacilla.org/fundamentals/whyprivacy.html> – Privacy Fundamentals
- [2] <http://www.news.com.au/story/0,23599,21073326-401,00.html> – Man wins \$500,000 in airline race profiling case
- [3] http://www.google.co.uk/mail/help/intl/en_GB/privacy.html – Google Mail privacy policy
- [4] Herman T. Tavani, Department of Philosophy, Rivier College, *Genomic research and data-mining technology: Implications for personal privacy and informed consent*, Ethics and Information Technology 6: 15-28, 2004
- [5] Helen Nissenbaum, University Center for Human Values, Princeton University, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, Law and Philosophy, 17: 559-596, 1998
- [6] Helen Nissenbaum, Berkshire Publishing Group, *Information Technology and Ethics*, Berkshire Encyclopedia of Human-Computer Interaction, 235-239, 2004
- [7] Mike Sharples, Educational Technology Research Group, University of Birmingham, *The Design of Personal Mobile Technologies for Lifelong Learning*, Computers & Education, 34 (2000) 117-193
- [8] I.B. Crabtree, S.J. Soltysiak, M.P. Thint, BT Laboratories, *Adaptive Personal Agents*, Personal Technologies Journal (1998) Vol. 2, No. 3, pp141-151
- [9] Raymond R. Burke, Indiana University, *Technology and the Customer Interface: What Consumers Want in the Physical and Virtual Store*, Journal of the Academy of Marketing Science, Vol. 30, No. 4, 411-432 (2002)
- [10] <http://www.usdoj.gov/oip/privstat.htm> – U.S. Privacy Act of 1974
- [11] <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> – Council of Europe – ETS no. 108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
- [12] <http://www.dataprotect.co.uk/dpa1984/> - Data Protection Act 1984 (c. 35)
- [13] Federal Trade Commission, *Online Profiling: A Report to Congress, Part 2 Recommendations*, July 2000
- [14] International Working Group on Data Protection in Telecommunications, *Common Position regarding Online Profiles on the Internet*, 27th meeting of the Working Group, 4/5 May 2000
- [15] <http://www.laptop.org/> - One Laptop per Child