A Projection of the Future Effects of Quantum Computation on Information Privacy and Information Security

Geoff Skinner, and Elizabeth Chang,

Curtin University of Technology, Perth, WA, AUSTRALIA

Summary
Many of the current issues with Information Privacy have been the result of inadequate consideration for privacy during the planning, design and implementation of Information Systems and communication networks. The area of Quantum Computation is still in its infancy, and a truly functional quantum computer has not been implemented. However, it is anticipated that within the next decade it may be feasible. This presents a unique opportunity to give due consideration to Information Privacy in the realm of future quantum computational devices and environments while they are still in their infancy. This paper provides an overview of the key Information Privacy issues that we feel may arise with the evolution and realization of quantum computation. Additionally we propose an integrated approach of technical, legal and social elements to address these issues.

Key words:
Information Privacy, Quantum Computation, Quantum Environments, TLC Privacy Protection.

Introduction

Recent research into the field of Quantum Computation has produced many interesting issues and alternative approaches to information and communication security. As with classical computer system evolution the new field of quantum computation is already at risk of following a similar path of overlooking information privacy concerns. Clarke [1] defines information privacy as being a combination of communications privacy and data privacy. He formally defines it as '… the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves' [1]. An individual's concern about their information privacy is a significant issue regardless of the technology used to .implement the information systems the entities are interacting with. It is widely regarded that many of the current information systems privacy inadequacies derive from the fact that privacy was never a serious consideration during the development life cycle of the systems [2]. This is in addition to the fact that the idea of privacy is itself very subjective in nature, unique to each individual and influenced by a broad range of factors from context to culture [3, 4]. From a financial perspective the ability to place monetary values on individual privacy is very difficult and therefore hard to integrate such factors into system design specifications and costing [5].

Modern privacy solutions are often derived from the application, both in combination and isolation, of the four main models of privacy protection [6]. The models are Comprehensive Laws, Sectoral Laws, Self Regulation, and Technologies of Privacy. Of interest to our own work is the impact of quantum computation on privacy enhancing technologies (PETs). The reason being is that many of the technology of privacy solutions rely on varying levels of computationally secure methods, such as encryption, to provide security and privacy of personal data [7]. With the advent of quantum computation and the possible realization in the near future of a quantum computer, many previous computationally secure methodologies will become redundant as they are tested in quantum networks and environments. For example the application of Shor's Algorithm [8] to find prime factors of a large number in polynomial time jeopardizes many cryptographic algorithms, such as RSA and PGP, many of which are used in privacy protection mechanisms.

While the advent of quantum computation does raise serious concerns to the effectiveness of many current privacy protection mechanisms, it is not all negative. Quantum computation also offers many advantages, which through its proper use, combined with other features of quantum mechanics and specific classical computational elements can be used to provide better privacy protection. Some areas currently under research and generating a lot of interest include quantum cryptography [9], Quantum based Private Information Retrieval (PIR) [10], Quantum anonymous transmissions [11], and quantum privacy amplification [12]. The focus of this paper is to provide a foundational perspective of our work investigating Information Privacy issues in the realm of quantum computation. We propose that solutions to address the increased privacy threats posed by quantum computation are similar to a degree of those required for current information privacy issues. That is, not only does Information Privacy conformance need to be integrated from system inception, but an effective privacy solution

Manuscript received August 5, 2006.
Manuscript revised August 25, 2006.

must be a symbiotic molding of technical, legal, and social elements.

The rest of the paper follows a common structure outline as follows. Section 2 provides relevant background material on Information Privacy for data at rest and in transit. Additional supplementary quantum computation areas are also discussed. Our research summary of a number of Quantum Computational technologies and their impact on Information Privacy is included in Section 3. Section 4 provides our proposals on what can be done to insure information privacy protection in Quantum Computational capable environments. A brief conclusion and future work is provided in Section 5.

2. Background and Related Work

Quantum Computation reaches its full potential when the operational environment is what is termed a quantum network. A quantum network consists of quantum computing devices representing the nodes connected with quantum communication lines [13]. As the topology of a network is abstracted from the technology of nodes and communication lines a number of security and privacy issues faced with classical networking environments are also applicable to quantum networks. While it is acknowledged that researchers still have a long way to go in understanding the potential and limitations of quantum computation, one group has a stated goal of building a "quantum Internet" [14]. So with the potential realization of quantum networks and a quantum Internet individuals are still faced with Information Privacy issues and questions about the privacy implications of the new technology. Our research aims to address these issues and find potential privacy benefits of quantum computation.

Quantum computation and the operational environment of quantum networks may inherent many of the same privacy issues that are faced by classical information systems and communication technologies [15]. However, it is the possibility that many unseen problems may be part of the new technology and therefore need investigation in respect to the quantum operational context. Our focus is on Information Privacy rather than Information Security, and specifically Privacy Enhancing Technologies [16]. The uniqueness of privacy in terms of its subjective nature and openness to individual interpretation and representation has allowed it to evolve with advances in technology, society, culture and values [17]. In the field of IS research privacy solutions are not always based on technological approaches. The use and enforcement of legal regulations, laws (sectoral and comprehensive), and even self regulation attempts will still be applicable to information privacy in quantum networks. However, protection against intentional malicious attacks is still heavily reliant on technological solutions. Therefore, when approaching information privacy issues in the age of quantum computation, our objective is to focus on the technological components.

According to the Common Criteria [18] privacy requirements for identity and privacy protection are concerned with anonymity, pseudonymity, unlinkability and unobservability. These set of requirements also provide a baseline level of protection requirements for privacy enhancing technologies (PETs). A major set of tools that facilitate these requirements is that of encryption. Encryption in general is used to protect information stored on a computer or transmitted over communication networks. By preventing access to data it also helps protect privacy. A number of PETs make extensive use of encryption in some form to help protect privacy. These include the Identity Protector [19], Privacy Shield [20], and Privacy Protector [21]. The form of encryption used is normally based on some form of Public Key Infrastructure (PKI), RSA, and other computationally hard (from a classical sense) algorithms. However, it has been shown that through the application of Shor's [8] work on factorization using quantum principles, many of the previous computationally secure encryption schemes can be compromised. Therefore any levels of privacy protection offered by PET's using encryption tools as part of their infrastructure will be in jeopardy. Another not so obvious threat to privacy with the advent of quantum computation is Grover's algorithm [22]. Basically this application of quantum principles dramatically decreases the amount of time it takes to search for a specific marked item in an unsorted database. Applied to many such data sources, in combination with advanced data mining and profiling algorithms, access and generation of personal profiles would be even more accessible.

With any new information technology with potential risks for privacy also come the potential for privacy benefits. The field of quantum computation is no exception. Perhaps the biggest advantage of the new technology is the fact it is so new. Being in its infancy allows system designers to hopefully learn from previous mistakes, in particular the design oversights of classical systems when considering information privacy. Privacy by design is a key concept that should be applied to all new information systems, whether they are classical or quantum in nature. Even hybrid combinations of both technologies can offer better privacy protection to the users of the systems. For example, while quantum computers are still some time away from general use, quantum cryptography over both classical and quantum communication networks has been achieved and commercial products are now available. [13, 14]. So while quantum cryptography may still provide no protection against "man-in-the-middle" attacks they do offer unsurpassed levels of encryption protection through their

creative application. For example, the classical Vernam code [23], which is unbreakable, has always suffered from key distribution problems. Through the application of quantum mechanical principles this issue is solved. The details are not provided here but may be found in [9]. What is important is the fact that information privacy benefited from such an application. Our work serves two purposes then. Firstly to highlight potential threats to information privacy and any advantages that may be gained from the quantum era we may soon be immersed in when applied to information privacy protection. Secondly, we propose some ideas to address the threats to privacy in the Quantum Era. We show that many of these solutions will require a unique molding of technical, legal and social elements to ensure information privacy is preserved.

3. Information Privacy in the Quantum Era

With space limitations of a publication papers the best approach to represent our work in progress is through the consideration of the key elements under investigation. This translates to consideration of key Quantum computational technologies that have either been realized or are still theoretical in nature. Discussion of each quantum technology is from an Information Privacy perspective in regards to potential threats to or and benefits for privacy. The topics included here are not a complete list but rather areas of particular relevance to Information Privacy issues that should be considered in a quantum network, whether realized or theoretical.

Quantum Computers and Shor's Algorithm: The central premise to quantum computing is the derivation and use of algorithms based on quantum mechanical properties in order to process information faster [13]. The algorithm that would represent the pinnacle of such research is one that provides an exponential speed increase. That is, solving a problem by quantum means in polynomial time, where it would normally take exponential time with classical computers. To date, the most useful proposed algorithm is the one developed by Shor [8]. Simply stated it would allow a quantum computer to find the prime factors of a large number in polynomial time. What would take a computational infeasible amount of time on a classical computer could be achieved in seconds on a quantum machine. The obvious threat here is that many modern encryption algorithms are based in this principle. That is, it would take an extraordinary if not impossible amount of time to find the prime factors of a very large number (RSA, PKI methods, etc). So infrastructures using these encryption algorithms for encrypting data at rest and transmitted over communication networks would be at risk. As a direct consequence any personal data included would be exposed and an individual's privacy compromised.

Quantum Computers and Grover's Algorithm: Like Shor's proposal Grover [22] has put forward an algorithm that takes advantage of quantum mechanical properties for processing speed increases. In this case it reduces the number of queries needed to search for a marked item in an unsorted database of N entries from N, classically, to about the square root of N, by quantum computation. Threats to information privacy may not be immediately evident until we consider applications such as data mining, profiling, and sharing of data from different organizations and data sources, such as data intelligence gathering. Many previous searches may have been seen as unfeasible, ineffective, or to costly use of resources as the time and number of queries needed to extract useful information was far too large. However, quantum computation and the use of Grover's algorithm have the potential to bring many of these searches into the realm of feasibility. As not all profiling and data mining is done with an individual's best interest in mind it represents a threat to information privacy and personal data protection. Many schemes that relied on anonymity or even pseudo-anonymity through obfuscation or hiding among large data sets may also be at risk for similar reasons.

Quantum Cryptography: Quantum cryptography relies on the laws of physics rather than various mathematical techniques to encrypt data. Classical cryptography, besides implementation of the Vernam cipher which has proved difficult and therefore impractical with classical implementation methods, can not guarantee absolute security of information. Therefore where that information is personal data it can not guarantee absolute privacy either. Quantum cryptography provides complete security of communication allowing two parties to exchange an enciphering key over a private channel. With secure key exchanges one time pads (Vernam) ciphers can be used to ensure both secure communication and privacy of any personal data communicated. It should be noted however that currently quantum cryptographic techniques are still susceptible to "man-in-the-middle attack" known as brigade attack. This issue is the focus of many research groups and there are positive signs for issue resolution.

Private Information Retrieval (PIR): PIR enables a user to retrieve an entry from a database, while hiding the index of the requested entry [10]. Through the use of quantum computation it has been shown that the communication complexity of PIR can be significantly reduced. A quantum PIR is characterized by a quantum server and communication over a quantum channel. The whole premise of PIR forms an important component of

privacy protecting systems. Quantum computation makes its use for feasible for the technology to widely available.

Anonymous Transmissions: Protocols used to hide the sender and recipient of message are known as anonymous transmission protocols. They provide another privacy protection tool in that they are able to hide the identities of entities involved in data exchanges. Many classical protocols of this nature are under threat with the advent of quantum computation for similar reasons most classical encryption methods are at threat. However, in [10, 11] a new quantum protocol has been proposed that provides anonymous transmission with perfect repudiation. Such a protocol ensures the future privacy of an entity's identity in a quantum computation environment.

Quantum Privacy Amplification: Privacy amplification is a sort of cryptographic version of error correction, which addresses some of the problems with the brigand attacks used on quantum cryptography. The idea is to start with long similar initial keys that the communicating parties assume an eavesdropper has some knowledge about. From these long keys the communicating parties make shorter shared random keys which are identical and unknown to an eavesdropper. It has been shown that quantum cryptography allows privacy amplification to be carried out directly, making it more efficient.

4. What Can Be Done?

Research to date strongly indicates that no single model of privacy protection is sufficient to provide a complete information privacy solution [6]. Therefore, we propose that a solution to this issue is to develop systems and operating environments that integrate a symbiotic molding of all four models of privacy protection. In addition, privacy by design and information system Hippocratic principles [2, 20] should be adhered to throughout the systems life cycle. To compliment the for-mentioned factors and provide robust information privacy protection architectures, the operating contexts [24, 25] as well as social and cultural environmental conditions need to be accounted for within the framework during development and deployment.

While technology achievements advance at a rapid rate, so to do the threats to privacy and an entities identity. Many PET's that have been proposed only deal with immediate threats to information privacy and do not look far beyond the current computational capabilities of systems and information processing environments. Not only are the computational abilities of systems increasing but also their level of ubiquity. Pervasive computing environments are becoming more common, and when coupled with increased computational capabilities dramatically increase the risks to information privacy. So in the event that quantum computation becomes feasible it will further place at risk entity privacy. Even early deployment of quantum computation capable systems, where perhaps only a central server may be quantum enabled, pose a serious threat to privacy. These central servers can be assigned dedicated tasks such as data profiling and mining, which if used maliciously, suddenly become privacy invasive technologies.

Any privacy solution must take into consideration all current and foreseeable future factors that pose a threat to information privacy. Therefore, we propose a solution entitled T.L.C. (Technical, Legal, and Contextual) Privacy Protection, referred to as TLC-PP. It is an approach that combines all four models of privacy protection [6], as well as consideration for the influence of social and cultural ideas and perceptions. It supports the implementation and methods of enforcement for both comprehensive and sectoral laws, self regulation and certification schemes, and the impact the operating context has on all of these components [26]. The TLC-PP objective is to address the issue of information privacy that is at risk from the increasing computational capacities of current and future computing environments. In particular, we are concerned with the possibility that in the near future quantum computational systems may be realized and soon become integral components of many computing environments. The diagram in Figure 1 provides a visual representation of the three TLC cornerstones of privacy protection and their respective components.

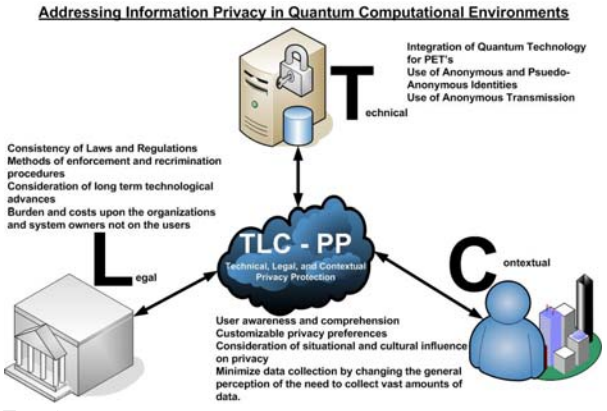

Fig. 1 The TLC model for Information privacy protection in Quantum Computational Environments.

Technological advances should be applied in equal measure to ensure privacy protection. With increased collection and processing of information it is imperative that industries and researchers contributing to

technological advances also develop complimentary methods of privacy protection. For example, as discussed in Section 3, with the advent of Quantum Computation there is the risk of compromising many of the widely used encryption technologies that help provide privacy protection. In order to offset this problem then it is possible to leverage the new technology to also provide better encryption methods such as the use of quantum cryptography. Additionally whether ever possible the use of anonymous and pseudo-anonymous identities should be used. This approach to identity and privacy protection can be abstracted from the technological implementation details. Therefore, no matter the computational capabilities of the computing environment, PET's should be in place that provides anonymous and pseudo-anonymous services. This also includes the use of anonymous transmission for network communications of private data, which coupled with quantum enhanced PIR (private information retrieval) can help ensure strong privacy protection.

Legal approaches to privacy protection have the advantage of being even further abstracted from technological advances. However, the need in the future will be to ensure consistency of privacy laws and regulations across all of globe. Equally important will be the ability to enforce the laws and regulations that are put in place. The burden and costs involved to pursue information privacy breaches should not be placed upon the user. Rather the onus should be on the system owners to ensure they correctly adhere to the privacy laws and regulations governing their operation. Currently the EU seems to be focusing on comprehensive privacy legislation rather than the sectoral approach seen in other countries and regions. Australia has made a number of promising steps towards improving their information privacy laws, however there still seems to be a lack of consumer awareness and organizational uptake. While this may be seen as a negative for current information privacy advocates at least one positive can be to be drawn from such a state. That is, it provides opportunities to incorporate measures that take into consideration future threats to information privacy such as the power of quantum computational environments.

Contextual conditions also play an important part in information privacy protection. Foremost of these initiatives should be the increasing social awareness of data collection and usage, and the need to protect their own privacy. Not all users or even cultures are the same when dealing with privacy. Certain societies and different contexts affect an entities need for and perception of privacy. Therefore, future systems need to not allow users to customize their privacy preferences based on different contexts, social and situational conditions [24]. Entities and system users should also be able to clearly understand and comprehend the privacy and data usage policies of the system they are using.

5. Conclusion and Future Work

With any new technology there is a much to learn often through trial an error. Privacy advocates are fortunate however in that many of the information privacy mistakes and issues that have been made with classical computing systems are ones that can be avoided or at least addressed with Quantum based systems. Privacy laws and regulations and self regulation are applicable to any information systems, regardless of the implementation technology. Our work is focused on the challenges faced to Information Privacy with the advent of quantum based technologies. We have discussed a number of key technologies and areas of quantum computational research in this paper. We have proposed a symbiotic molding of various privacy protection models into an approach we have termed TLC-PP (Technical, Legal, and Contextual Privacy Protection).

TLC-PP incorporates many components and elements that affect information privacy. The TLC-PP approach caters for advances in computational processing capabilities of future systems, in particular the possible realization of quantum processing environments. Our ongoing work encompass many other quantum computational developments as they impact upon information privacy, whether is in a negative or positive way. An important objective of the research is to highlight the need for Information Privacy awareness from an early development stage for quantum computational systems and protocols. This can be further achieved by the integration of privacy by design principles

References

[1] R. Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html, September, 1999.

[2] G. Skinner and E. Chang, "PP-SDLC The Privacy Protecting Systems Development Life Cycle", IPSI-2005 FRANCE, April 23 till April 26, 2005.

[3] Yingxin (Sheila) He, Dawn N. Jutla, "Contextual e-Negotiation for the Handling of Private Data in e-Commerce on a Semantic Web," HICSS, p. 62a, Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) Track 3 (2006).

[4] R. Wishart, K. Henricksen, and J. Indulska, "An access control scheme for ubiquitous computing environments based on context-dependent privacy preferences", ACISP

2005, The 10th Australasian Conference on Information Security and Privacy, Brisbane Australia, 4-6 July, 2005.

[5] S. Faja, "Privacy in E-Commerce: Understanding User Trade-Offs", Issues in Information Systems, Volume VI, No. 2, 2005.

[6] EPIC, "Privacy and Human Rights 2003", Electronic Privacy Information Centre, http://www.epic.org

[7] G. Skinner, S. Han, and E. Chang, "The Computational View of Information Privacy for Privacy Enhancing Technologies", The First International Conference on Legal, Security and Privacy Issues in IT (LSPI), 2006.

[8] P.W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", Proceedings of the 35th Annual Symposium on Foundations of Computer Science, USA, Nov. 20-22, 1994.

[9] C. H. Bennett, G. Brassard, "BB84", Proc. IEEE International Conference on Computers, Systems, and Signal Processing, IEEE Press, Los Alamitos, Calif. (1984), p. 175.

[10] S. Wehner, "Quantum Computation and Privacy", Master's Thesis in Theoretical Computer Science, Universiteit van Amsterdam, 2004.

[11] M. Christandl and S. Wehner, "Quantum Anonymous Transmissions", Proc. of 11th ASIACRYPT, 2005, LNCS 3788, pages 217-235.

[12] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels", Physics Review Letters. 1996 Sep 23;77(13):2818-2821.

[13] G. Giedke (MagiQ), "What is Quantum Information Processing", http://www.magiqtech.com/index.php.

[14] S. Robinson, "Gauging the Limits of Quantum Computing", The New York Times On The Web, March 7, 2000.

[15] IBM Research Report, "Views of Privacy: Business Drivers, Strategy, and Directions", IBM Research Division, Sept., 2003.

[16] I. Goldberg, "Privacy-enhancing technologies for the Internet II: Five years later", PET 2002, San Francisco, 2002.

[17] R.M. Davison, R. Clarke, J. Smith, D. Langford, and B. Kuo, "Information Privacy in a Globally Nteworked Society: Implications for IS Research", Communications of the Association for Information Systems, Volume 12, 2003, 341-365.

[18] Common Criteria Project, "The Common Criteria", http://www.commoncriteriaportal.org/.

[19] G.W. van Blarkom, J.J. Borking, and J.G.E. Olk, "Handbook of Privacy and Privacy-Enhancing Technologies", Privacy Incorporated Software Agent (PISA) Consortium, The Hague, 2003.

[20] G. Skinner and E. Chang, "A Conceptual Framework for Information Privacy and Security in Collaborative Environments", International Journal of Computer Science and Network Security, Vol. 6 No. 2B, Feburary 28, 2006.

[21] D.A. Gritzalis, "Embedding privacy in IT applications development" Information Management and Computer Security, Vol. 12 No. 1, 2004.

[22] L. Grover, "Quantum Mechanics helps in searching for a needle in a haystack", Physics Review Letter. 79, 325 (1997).

[23] Protechnix, "Cryptology and Data Secrecy : The Vernam Cipher", http://www.pro-technix.com/information/crypto/pages/vernam_base.html.

[24] G. Skinner and E. Chang, "Fair Privacy Principles and Preferences (F3P) – Evaluating Context Based Privacy Preferences", The 10th WSEAS International Conference on Computers, ICCOMP-06, Vouliagmeni, Athens, Greece, July 13-15, 2006.

[25] M. Ackerman, T. Darrell and D.J. Weitzner, "Privacy In Context", MIT Discussion Paper, http://www.eecs.umich.edu/~ackerm/pub/01a12/context-privacy.final.pdf.R. Clarke, "Introduction to Dataveillance and Information Privacy, and Defintions of Terms", http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html, September, 1999.