IGI PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

ITJ3794

This paper appears in the publication, **International Journal of Information Security and Privacy**, Volume 1, Issue 3
edited by **Hamid R. Nemati © 2007, IGI Global**

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

Geoff Skinner, Centre for Extended Enterprise and Business Intelligence Curtin University of Technology, Australia

Elizabeth Chang, Centre for Extended Enterprise and Business Intelligence Curtin University of Technology, Australia

ABSTRACT

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 article 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.

Keywords: *data security; Internet privacy; privacy laws; privacy regulations*

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 (1999) 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" (Clarke, 1999). 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 of the systems (Skinner & Chang, 2005). 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 (He & Jutla, 2006; Wishart, Henricksen, & Indulska, 2005). From a financial perspective the ability to place monetary values on individual privacy is very difficult and therefore it is hard to integrate such factors into system design specifications and costing (Faja, 2005).

Modern privacy solutions are often derived from the application, both in combination and isolation, of the four main models of privacy protection (EPIC, 2003). 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 (Skinner, Han, & Chang, 2006). 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 (Shor, 1994) 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 (Bennett & Brassard, 1984), quantum-based private information retrieval (PIR; Wehner, 2004), quantum anonymous transmissions (Christandl & Wehner, 2005), and quantum privacy amplification (Deutsch, Ekert, Jozsa, Macchiavello, Popescu, & Sampera, 1996). The focus of this chapter 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 must be a symbiotic molding of technical, legal, and social elements.

The rest of the chapter follows a common structure outline as follows. The next section provides relevant background material on information privacy for data at rest and in transit. Additional supplementary quantum computation areas are also discussed. The next section provides a number of quantum terms defined for the context of our work, in addition to applicability to information privacy. Our research summary of a number of quantum computational technologies and their impact on information privacy is included in the section that