1996

The age of smart cards: an exploratory investigation of the sociotechnical factors influencing smart card innovation (1974-1996)

Robyn Alice Lindley
University of Wollongong

The age of smart cards: an exploratory investigation of the sociotechnical factors influencing smart card innovation (1974-1996)

Robyn Alice Lindley
University of Wollongong

The Age of Smart Cards:

An exploratory investigation of the sociotechnical factors influencing smart card innovation (1974-1996)

A thesis submitted in fulfilment of the requirements for the award of the degree

Doctor of Philosophy

from

The University of Wollongong

by

Robyn Alice Lindley, B.Sc. (Sydney University)
Grad. Dip. Ed. (Sydney University)
M.Info.Tech. (University of Wollongong)

Department of Information and Communication Technology

Declaration

This thesis is submitted in accordance with the regulations of the University of Wollongong in partial fulfilment of the requirements for the award of a Doctor of Philosophy. It does not incorporate any material previously published or written by another person except where due reference is made in the text. The work described in this thesis is original work and has not been previously submitted for a degree or diploma in any university.

Robyn A. Lindley

April, 1996

"As technologies become more complex and flexible in their application, so must people become more competent and empowered in their response."

(Taylor and Felton, 1993: 205)

Abstract

This thesis breaks new ground by providing the first detailed study of smart card innovation during its first twenty years (1974-1996). The overall aim is to apply sociotechnical principles to further our understanding of the innovation process as it relates to smart card technology. By using a sociotechnical framework, this study also seeks to illustrate the limitations of conventional innovation theory when applied to new information technologies such as smart card: The central thesis posited, is that to develop our understanding of the underlying innovation processes that have occurred during the development of this new information technology, it is necessary to study the interactions between three actors that have all appeared to play a role in the process of smart card innovation. These are smart card technology; the potential users and the organisations. However, in stating this, it is also important to realise that one tacit assumption underlying the work reported here is that new technologies are only adopted if the technological parameters (technology focus), the market needs (user focus) and the entrepreneurs (organisational focus) meet.

At a more abstract level, the work has also endeavoured to consider whether a sociotechnical approach applied as a framework for understanding the process of innovation for smart card is, in fact, a reasonable and useful paradigm for developing our understanding from both a theoretical and applied perspective. Thus the multidisciplinary process approach adopted is not intended to lead to a complete alternative theory: nor is it intended to be merely a synthesis.

What the current work has achieved, is to provide the very first insights into the understanding of smart card innovation. The sociotechnical framework adopted as a theoretical organiser and, which emphasises the role of the user, has also served to

highlight the need for a multidisciplinary approach to develop our understanding of smart card innovation. The view upheld is that the paradigm emerging from these analyses based on traditional innovation thought, both demands and empowers the view of smart card innovation as a sociotechnical process. One of the main outcomes has been to demonstrate that smart card innovation provides a case in point highlighting the benefits of adopting a broad and evolutionary approach to innovation and based on a sociotechnical framework. This is in agreement with recent paradigm shifts in technology innovation thought. For the practitioner, these findings also illuminate new possibilities for the development theoretically informed smart card systems, thus placing the smart card design team in a position to significantly and positively influence future smart card innovation patterns.

Acknowledgments

The time spent gathering the data and information presented in this thesis was a rewarding experience. This is in no small way due to the support and involvement of my supervisor, Professor Joan Cooper. I would like to thank Joan for her continued support and for giving me the opportunity to experience different facets of the academic process of inquiry. I would also like to thank my colleague Dr Leone Dunn for her support and encouragement during the final stages of the studies reported.

Contents

Contents

Contents

Contents

Contents

Tables

Tables

Figures

Figures

Figures

Abbreviations

ADF	Application Data File
AES	Associated Electronic Services (Australia)
AFC	Automatic Fare Collection
AID	Alternate Identification File
AK	Authentication Key
AIM	Advanced Informatics in Medicine program of the Commission of European Communities.
ANSI	American National Standards Institute
ASS	Allterminal Security layer Specification (developed by the Swedish Agency for Administrative Development)
ATEA	Australian Telecommunications Employees Association (ATEA)
ATM	Automatic Teller Machine
AVI	Automatic Vehicle Identification
B-ISDN	Broadband ISDN
CAD	Card Acceptor Device
CASC	Comprehensive Analysis for Smart Card (basic design approach)
CCTV	Closed Circuit Television
CD	Compact Disc
CDF	Common Data File
CDK	Ciphering/Deciphering Key
CEN	*Comite Europeenne de Normalisation* (European Standards Organisation)
CEPT	*Conference Europeenne des Administrations des Postes et Telecommunications* (European Committee for Post and Telecommunictation Standards)
CK	Ciphering Key
CLI	Calling Line Identification
CMOS	Complementary MOS technology
Co-Co	Coordination of the primary care information network (an EU telematics project)
CPS	*Carte de Professionelle de Sante* (French Health Professional Card)
CPU	Central Processing Unit of a microprocessor
DEC	Digital Equipment Company
DES/DEA	Data Encryption Standard/Algorithm
DF	Data File
DIABCARE-Q-NET	Quality network for the care of diabetic patients (an EU telematic network project)
DK	Deciphering Key
DRAM	Dynamic RAM
DS	Digital Signature
DSA	Digital Signature Algorithm
EAA	Export Administration Act (US)
EC	(The) European Community
ECMA	European Community Manufacturers' Association
EDI	Electronic Data Interchange

Abbreviations

EDIFACT	European Committee for Information Technology & Telecommunications Testing and Certification (a program to achieve pan-European recognition of testing performed by certified laboratories)
EDL	Electronic Drivers Licence
EES	Electronic Exponential Signature
EEPROM	Electronically Erasable Programmable Read Only Memory (memory used for data storage or for volatile data storage)
EFT	Electronic Funds Transfer
EFTPOS	Electronic Funds Transfer at Point of Sale
EHTO	European Health Telematics Observatory
EK	Erase Key
EPROM	Erasable Programmable Memory. The memory is used to store application programs.
ES	Electronic Signature
ETSI	European Telecommunications Standard Institute
EU	European Union
FRAM	Ferro-electric Random Access Memory (enables smart cards to retain information without a battery)
GMPTE	Greater Manchester Passenger Transport Executive (public transport authority in Greater Manchester, UK)
GNP	Gross National Product
GP	General Practitioner
GSM	Global Standard for Mobile Communications
GVE	RA software tool developed by Daimler-Benz AG of Berlin
HCMOS	High Density, Low Power MOS technology
HIV	Human Immune deficiency Virus
IC	Integrated Circuit
ICC	IC Card
ICCP	Information Computer and Communications Policy (OECD Committee for security of information systems)
IK	Issuer Key
INFOSEC	Swedish Institute for Health Services R&D Program in the area of IT Systems Security and Information Security
IPR	Information Privacy Rights
IR	Infra Red
IS	Information Systems
ISDN	Integrated Services Digital Network
I/O	Input/Output lines
ISO	International Organisation for Standardisation
IT	Information Technology
ITSEC	The European Information Technology Security Evaluation Criteria
MAP	Modular Arithmetic Processor
MASK	Medium used to convert customers application software to a pattern in the silicon which can be read (ROM code).
MCU	A Single Chip Microcomputer is often referred to as an MCU.
ME	Mobile Equipment

Abbreviations

MFC	Multifunction Card
MFC/O	MFC operating in an Open systems environment
MOS	Metal Oxide Semiconductor technology
MS	Mobile Station
NMOS	N-channel Metal Oxide Semiconductor technology
NSA	National Security Agency (US)
NVM	Non-Volatile Memory (for permanent memory storage)
OCR	Optical Card Reader
OECD	Organisations for Economic Co-operative Development
PC	Personal Computer
PCMCIA	PC Memory Card Industry Association
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PLANEC	Planning of the care of the elderly in the EU (telematics project)
PROM	Program Read Only Memory (data can be altered once the card is in use)
POS	Point of Sale
PTT	Post Telephone and Telegraph
PVC	Polyvinyl Chloride (used to manufacture smart cards)
QR	Qualitative Reasoning
RA	Risk Assessment
RAM	Random Access Memory (RAM used as temporary working memory. It is lost when the card loses power.)
R&D	Research and Development
REMEDES	*REseau Multimedia Europeens pour Doctuers et Etablissements de Sante*
RF	Radio Frequency
RISC	Reduced Instruction Set Computer
ROM	Read Only Memory (Installed by manufacturer of the microprocessor chip and the information it contains is the operating system - often called a template or *masque*. It cannot be altered.)
RSA	*Rivest - Shamir - Adleman* encryption algorithm
SIM	Subscriber Identity Module (used to identify the caller on a GSM network)
SC	Smart Card (ISO standard card embedded with a MCU)
SCT	SC Terminal (communications)
SMEG	Monetary Systems Engineering Group (research group at the University of Newcastle, Australia)
SPRI	Swedish Institute for Health Services Development
SRAM	Static RAM
SVC	Stored Value Card
TQM	Total Quality Management
VCR	Video Cassette Recorder
VME	Visa-Mastercard-Europay
WORM	Write Once, Read Many times optical disc