DesktopWitness

the do's and don'ts of
personal computer security

Michael A. Caloyannides

Desktop Witness

The do's and don'ts of personal computer security

Michael A. Caloyannides

Senior Fellow
Mitretek Systems
Virginia, USA

JOHN WILEY & SONS, LTD

 John Wiley & Sons Ltd,
Baffins Lane, Chichester,
West Sussex PO19 1UD, England
National 01243 779777
International (+44) 1243 779777
e-mail (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on http://www.wileyeurope.co.uk

Library of Congress Cataloging-in-Publication Data
(applied for)

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0 471 48657 4

Typeset in $10\frac{1}{2}/12\frac{1}{2}$pt Sabon by Keytec Typesetting, Bridport, Dorset
Printed and bound in Great Britain by Biddles Ltd., Guildford and Kings Lynn
This book is printed on acid-free paper responsibly manufactured from sustainable forestry,
for which at least two trees are planted for each one used for paper production.

Desktop Witness

Dedication

This book is dedicated to my parents, Akylas and Etta, who considered the raising of their children to be their highest priority, and to my two infant children Melody and Brian whom I will not live to see as grown up adults as I am now battling lymphatic cancer. Hopefully, they will carry the torch of individual freedom in a world increasingly opposed to it.

Preface

When asked 'who are you?', people in different cultures tend to define themselves fundamentally differently in terms of what their respective culture considers to be most important. In cultures where one's professional and economic status is most important, people say 'I am an engineer', or 'a priest at St John's church', or whatever one's profession is. In cultures where family ties and ancestry are most important, people say 'I am John's son', or 'Hsiu's grandson'. Hardly anywhere does one answer the 'who are you?' question by asking 'in what context?'; societal pressures in most societies force most individuals to have largely one-dimensional personas.

The all too human yearning for security and for acceptance by others often makes some of us internalize and accept our immediate community's prevailing standards and beliefs as gospel without using any of our own judgment, and viewing with suspicion those that dare question those beliefs. Most in pre WWII Germany accepted Nazism because it was the 'in' thing; similarly, most ruthless dictators have a considerable number of followers, and so do most quasi-charismatic leaders of assorted oddball cults even if some of these leaders have mesmerized their followers into committing mass suicide – as has happened time and again.

The yearning by most people to have someone else 'spoon-feed' them what is 'right' and what is 'wrong', and to relieve them of the burden of deciding that for themselves, is, I believe, very strong for most people. It is no surprise, then, that the notion of privacy for others (as opposed to privacy for oneself) is very threatening to many; after all, it implies that someone else may have different views – God forbid – and that privacy may get in the way of the rest of the community knowing that!

For related reasons, citizen privacy is certainly threatening to most any government because it could keep dissent from being identified and being nipped in the bud. Even democratically elected governments that pride themselves in their purported respect for citizen privacy have a catch-all exclusion such as 'except as lawfully authorized ...'. In short, privacy is OK as long as you believe what the state (or the community) believes. Stated differently, you can choose any color as long as it is the one that is approved.

Having been born and raised in one culture, educated and lived my professional life in another, being married to a wonderful woman from a third culture, and having adopted a child from yet a different culture, I have come to appreciate the fact that a perspective that seems unpalatable to one culture (say, to law enforcers) makes perfectly good sense if seen within the logic framework of a different culture (say, freedom fighters in an oppressive regime). As such, I was not about to write a book preaching any party line, nor a book that is intended solely for one or the other point of view. Instead, this book is intended for anyone who is mature enough to value privacy. Sadly, this is not everyone, although most everyone values his or her own privacy – but not anybody else's.

Although this book deals with some fairly esoteric topics, it is intended to be understandable by anyone with intelligence. Quite simply, this book is for free-thinking, responsible, and mature people who want to write, store, and communicate their ideas with privacy. This includes businesspeople with proprietary documents, physicians with confidential data on patients, philosophers with new ideas, freedom fighters in oppressive regimes, and any person in need of privacy.

This book is for responsible people in need of safeguarding their privacy when using the twenty-first century's primary tool, namely, a computer of some sort. It is *solely* for responsible and mature people, and not for crooks; as with a kitchen knife or a screwdriver, a computer can be used for good and it can be used for evil. This book is emphatically not intended to facilitate the latter.

Gross abuse of anonymity is criminal, unconscionable, unethical, despicable, and shameful. There have been far too many documented cases when individuals' lives have been ruined as a result of anonymous malicious messages to their family, neighbors, employers, and friends. This conduct is positively not what this book is in any way condoning; quite the contrary, such malice should be hunted down and prosecuted.

No sane person is pro-arson or pro-murder, but one should not allow any oppressive regime's self-serving habit of criminalizing every act that it does not like to shape one's own judgment of what is really right or wrong. As an example of some 30 years ago, a military junta in Greece, the birthplace of democracy, banned the study of some ancient Greek philosophers because they talked 'too much' about freedom. Such practice is wrong regardless of what the self-serving laws in the oppressive regime say.

It used to be that the ultimate threat to privacy was some caricature of an authority figure in an oppressive regime, in or out of uniform. It also used to be that just as real a threat was the classical neighborhood 'busybody', that is, the immaturity and intolerance of our neighbors, of our social acquaintances, and of the people that we interfaced with. It was they who would feel threatened enough by our nonconformist views and conduct to consider it their 'obligation' (to whom?) to report to 'the authorities'. Today, conducting ourselves with discretion

is not enough. Technology, such as interception of online traffic, makes the possibility of wholesale surveillance and automated screening not only possible but already in place. Unless one has nothing creative to offer beyond regurgitating the local dogma, one needs effective means of staying out of any oppressive regime's – and even out of one's neighbors – 'radar screens'.

One should also keep in mind that, even under the best of circumstances when one has done nothing wrong, law enforcement databases in even the most technologically advanced country often contain major errors. According to *Wired* reporter Julia Stevens on 11 May 2001 (http://www.wired.com/news/privacy/0,1848.43743,00.html), 'when Richard Smith got his FBI file, he learned ... that he had died in 1976 and that he may have been previously married to a woman named Mary ... [and] that he may be known [by] aliases he shares with a couple of convicts doing hard time in Texas'.

Perhaps unwisely, in this book I call a spade a spade, with no deference towards corporations or governments. Inevitably, this candor will offend some corporations and governments. I fully expect this book to be banned in some countries and attempts to be made to discredit it – and me.

In the final analysis, when we lie on our deathbeds we have to seek acceptance by a most critical and unforgiving evaluator of our lives who will see right through any excuse: our own individual conscience.

Michael A. Caloyannides
Washington, DC, January 2002

Acknowledgement

All patents and trademarks are hereby acknowledged as the property of their respective owners.

Contents

1

The Need is Very Real: Author's Perspective

Security is the means by which one makes it difficult for another forcibly to obtain information, whereas privacy is the means by which one makes information unavailable. Privacy and anonymity have been taken for granted in daily life since time started. We buy groceries and movie tickets with cash, we browse at store windows without showing any identification, and we look at newspapers without anyone knowing which particular article we are reading. Lovers have always whispered sweet words in each other's ears in private, and even some formal written and oral communications – such as privileged discussions between lawyer and client – have enjoyed legally sanctioned confidentiality in civilized societies.

This is all changing very rapidly simply because technology makes it easy to break confidentiality. The incentive to violate individuals' privacy exists both in commercial and in government sectors. Commerce has realized the cost-effectiveness of directed advertising to those already known to have an interest in what is being peddled, and has been deploying increasingly sophisticated technical means of identifying who likes what. Repressive governments, which have always feared any dissent, have availed themselves of even more intrusive technologies to create and maintain vast databases about people in order to identify any and all dissent so as to nip it in the bud; sadly, even democratic governments have played up citizens' insecurities and have done the same under the guise of protecting us from each other. One should not forget Montesquieu's words: 'there is no greater tyranny than that which is perpetrated under the shield of law and in the name of justice'. Nor should we forget the words of William Pitt, British Prime Minister, on 18 November 1783: 'Necessity is the plea for every infringement of human freedom; it is the argument of tyrants; it is the creed of slaves'. It is perilous to assume the position that 'I have done nothing wrong, so I am safe'. Holocaust victims had done nothing wrong either but had a lot to fear, and the same is true for numerous executed individuals who have been exonerated post-mortem as a result of DNA testing.

Furthermore, privacy is an essential element of freedom and does not imply any wrongdoing. We shower in private, we try to keep our medical records private, and