8 In conclusion…

The wave of rapid innovation of the last 10 years shows no signs of slowing down and attempting to predict which developments will be successful is a matter for gamblers willing to invest in promising consumer oriented initiatives and see what happens.

Where such innovations will take society is another unpredictable topic. What we should have learned by now is that the ease of use of such products hides a great deal of complexity, and this, in turn, the reality that all such products contain imperfections – the author refers to them as "bugs" while some of the designers call them "features".

This is understandable when we consider the many parties involved in delivering innovative technologies. Looking at smartphones for example, they require the fusion of the work of:

- Hardware designers and manufacturers – processors, storage, screens and so on
- Operating system designers – the essential software that makes the device work
- Application designers – ranging from large software houses to single individuals
- Service providers – offering voice and data service contracts, sometimes adding apps to the devices they retail
- WiFi Hotspot providers – including shops, hotels and restaurants offering WiFi services, sometimes free of charge
- Device assemblers usually in low wage economies

All of the above work independently of each other and deal with devices of such complexity that no amount of testing prior to production can identify 100% of the possible vulnerabilities and bugs. This complexity is hidden from the end user. When this person is unaware of how to protect the device and the data it contains, disappointment, frustration and headaches are likely outcomes.

To this, we need to add the context in which some of the above activities are carried out:

- The role of venture capital and expectations of a rapid return on investment, which drives time to market
- The entrepreneurial ambition of becoming a millionaire by age 25 and a billionaire by age 40, often involving an Initial Public Offering (IPO)
- The technically highly skilled developers that sometimes lack empathy or concern for the end user
- The pressure to reduce costs

And finally those for whom this book is intended: The individuals that have not thought about the many vulnerabilities associated with new devices and therefore are unaware of:

- Good digital hygiene practices and don't know what should be done
- Why it should be done
- How it should be done

Then there are those who don't want to know and don't really care (until things go wrong).

What you should do about it

To the readers that got this far, thank you for your patience. This book has 39 sections describing generally accepted good practices. Many of them are simple and quick to apply and Chapter 3 lists those considered to be the ones to start with.

Chapter 4 presents items to reflect on and implementing them may require the reader to change their approach to disclosures, assess how much privacy they wish to retain and become aware of the many parties interested in their personal data.

Chapter 5 describes the main landmines you are likely to encounter in cyberspace and describes how to avoid them – if they appear as restrictions, it is because they are. The precautionary principle of "better safe than sorry" should be considered good advice.

Chapter 6 describes somewhat more advanced things to do. Not necessarily the highest priority but it's good to be aware that once implemented, you can feel more secure.

Chapter 7 is an attempt to predict how things under development now may impact on our social and personal life. As Nobel Prize Niels Bohr is alleged to have said "it is difficult to make predictions particularly about the future". There are so many developments towards what is generally known as The Internet Of Things that trying to predict which will become a successful product is no more than a gamble.

Chapter 9 presents a short list of other publications addressing the same issues and websites that provide good guidance. The list is nowhere complete but consists of trustworthy sources.

Is this book a complete guide to good digital hygiene?

Certainly not, and to a large extent deliberately so as publishing guidelines running to hundreds of pages would be a deterrent to getting started. Two domains beyond the author's knowledge and experience are:

Protecting children in cyberspace: this would include the effective use of parental controls, guidance on potential predators, online purchases, unsuitable sites, disclosures, addiction to video games and so much more. Such guidelines are available thorough the use of a search engine and government issued guidelines should be considered reliable.

Cybersecurity for Silver Surfers: in Europe there are constant reminders about the changing age profile of the population as life expectancy increases and these Silver Surfers have to accept that initiatives in e-government, facilities such as online video and audio telephony, e-commerce and so on have left them no option but to use the World Wide Web and mobile devices. From personal experience from older friends, it is clear that their level of awareness of cybercrime, malicious software and other risks is low. It is also difficult to try to explain these things in a way that makes sense to them.

Can we learn anything from the past that points towards the future?

Those of us who enjoy the creative ideas of science fiction writers and film makers should recall that there are many books, magazine articles and movies on how future technologies will impact society. Many were written well before such technologies (perhaps their research was inspired by their ideas) became available. Here are a few examples:

- The concept of geostationary satellites, by Arthur C. Clarke in a communication to the editor of Wireless World (1945) – followed by many other ideas (see 2001 below)
- Nineteen Eighty Four, by George Orwell (1949) – on an intrusive state that monitors individuals and more
- I, Robot, a series of short articles by Isaac Asimov (1950)
- 2001 (movie) – released in 1966 – in which an artificial intelligence computer named HAL who communicates in natural language decides that completing its mission requires it to dispose of the astronauts
- Star Trek – the original TV series, 1966 to 1969 in which a "communicator" is used. Many cellular phones (shell phones or flip fold models) currently available look almost identical to it
- Cyborg, book by Martin Caidin, 1972. Provides the basis for the TV series The Six Million Dollar Man 1974 to 1978 where a former astronaut is "rebuilt" using bionic implants. This theme has been used in several other TV programs and movies since
- Star Trek – The New Generation TV series 1997 to 1984 where the computer communicates in natural language, touch screens and devices that look very much like tablets are in evidence. Advanced medical electronics, universal translators, etc. are also shown

This list could be extended considerably. The main lesson that can be drawn from it is that the creative ideas of the world of fiction can successfully migrate to the real world – it may take many years and many failures. The impact of successful initiatives on society and individuals can introduce significant change as well as undesirable and unpredictable side effects.