# PART ONE

## PROLOGUE

ONE

# Introduction

A few years ago I attended an event where the guest speaker was a Cabinet member. In conversation afterwards, the subject of long-term petroleum supplies came up. He warned that at some point, perhaps a century or so in the future, someone would put his key in his car's ignition, turn it, and nothing would happen – because there would be no gasoline.

What shocked me was not his ignorance of the economics of depletable resources – if we ever run out of gasoline it will be a long, slow process of steadily rising prices, not a sudden surprise – but the astonishing conservatism of his view of the future. It was as if a similar official, 100 years earlier, had warned that by the year 2000 the streets would be so clogged with horse manure as to be impassable. I do not know what the world will be like a century hence. But it is not likely to be a place where the process of getting from here to there begins by putting a key in an ignition, turning it, and starting an internal combustion engine burning gasoline.

This book grew out of a seminar on future technologies that I taught for a number of years at the law school of Santa Clara University. Each Thursday we discussed a technology that I was willing to argue, at least for a week, could revolutionize the world. On Sunday, students emailed me legal issues that that revolution would raise, to be put on the class web page for other students to read. Tuesday, we discussed the issues and how to deal with them. Next Thursday a new technology and a new revolution.

The idea for the course started with two then obscure technologies: public key encryption and nanotechnology. As the course developed I

found myself exploring a considerable range of others, with one feature in common: Each might change the world within my lifetime. What you are reading is an exploration of those technologies, the futures each might generate, and how we might deal with them. This chapter briefly surveys the technologies; the next discusses the problem of adjusting our lives and institutions to their consequences.

At the moment, the fashionable focus for worries about the future is global warming. It is probably a real problem and perhaps something should at some point be done about it. But, despite all the public furor and images of flooded cities, on current evidence it is not a very large problem. The latest estimates from the United Nations International Panel on Climate Change (IPCC) predict, if nothing is done, a sea level rise of a foot or two by the end of the century, an increase in average temperature of a few degrees, and perhaps a small increase in the frequency and force of hurricanes. It is possible that those predictions will turn out to be far too modest, but they are what we currently have to work with.

At least three of the technologies I discuss in this book – nanotech, biotech, and artificial intelligence (AI) – have the potential to wipe out our species well before the end of the century. They also have the potential to create a future sufficiently rich and technologically advanced to make global warming a problem that can be solved at the cost of the spare cash of a few philanthropists. Other technologies might create futures strikingly different from the present in a wide variety of ways: a radically more, or radically less, free society than we now live in, more privacy than humans have ever known or less, humans living like gods or like slaves. Their consequences will affect not only law but marriage, parenting, political institutions, businesses, life, death, and much else.

I am not a prophet; any one of the technologies I discuss may turn out to be a wet firecracker. It only takes one that does not to remake the world. Looking at some candidates will make us a little better prepared if one of those revolutions turns out to be real. Perhaps more important, after we have thought about how to adapt to any of ten possible revolutions, we will at least have a head start when the eleventh drops on us out of the blue. The conclusion I want readers to draw from this book is not that any one of the futures I sketch is going to happen. The conclusion I want them to draw is that the future is radically uncertain. In interesting ways.

And that it is worth starting to think about the possibilities, and how to deal with them, now.

## POSSIBLE FUTURES

We start with three technologies relevant to privacy – one that radically increases it, two that radically decrease it.

### Privacy x 3 or

***Now You Have It, Now You Don't***

Public key encryption makes possible untraceable communications intelligible only to the intended recipient. My digital signature demonstrates that I am the same online persona you dealt with yesterday and your colleague dealt with last year, with no need for either of you to know such irrelevant details as age, sex, or what continent I am living on. The combination of computer networking and public key encryption makes possible a level of privacy humans have never known, an online world where people have both identity and anonymity – simultaneously. One implication is free speech protected by the laws of mathematics, arguably more reliable and certainly with broader jurisdiction than the Supreme Court. Another is the possibility of criminal enterprises with brand-name reputation – online pirate archives selling other people's intellectual property for a penny on the dollar, temp agencies renting out the services of forgers and hit men.

***On the Other Hand . . .***

In the not-too-distant future you may be able to buy an inexpensive video camera with the size and aerodynamic characteristics of a mosquito. Even earlier, we will see – are already seeing – the proliferation of cameras on lampposts designed to deter crime. Ultimately, this could lead to a society where nothing is private. Science fiction writer David Brin has argued that the best solution available will be not privacy but universal transparency – a world where everyone can watch everyone else. The police are watching you – but someone is watching them.

It used to be that a city was more private than a village, not because nobody could see what you were doing but because nobody could keep track of what everybody was doing. That sort of privacy cannot survive

modern data processing. The computer on which I am writing these words has sufficient storage capacity to hold at least a modest amount of information about every human being in the United States and enough processing power to quickly locate any one of those by name or characteristics. From that fact arises the issue of who has what rights with regard to information about me currently in the hands, and minds, of other people.

Put all of these technologies together and we may end up with a world where your realspace identity is entirely public, with everything about you known and readily accessible, while your cyberspace activities, and information about them, are entirely private – with you in control of the link between your cyberspace persona and your realspace identity.

## Commerce in Cyberspace

The world that encryption and networking create requires a way of making payments – ideally without having to reveal the identity of payer or payee. The solution, already worked out in theory but not yet fully implemented, is ecash – electronic money, privately produced, potentially untraceable. One minor implication is that money laundering laws become unenforceable, since large sums can be transferred by simply sending the recipient an email.

A world of strong privacy requires some way of enforcing agreements; how do you sue someone for breach of contract when you have no idea who, where, or what he, she, or it is? That and related problems lead us to a legal technology in which legal rules are privately created and enforced by reputational sanctions. It is an ancient technology, going back at least to the privately enforced *Lex Mercatoria* from which modern commercial law evolved.[1] But for most modern readers, including most lawyers and law professors, it will be new.

Property online is largely intellectual property, which raises the problem of how to protect it in a world where copyright law is becoming unenforceable. One possibility is to substitute technological for legal protection. A program or database comes inside a piece of software – Intertrust called it a digibox – that regulates its use. To run the program or query the database costs ten cents of ecash, instantly transmitted over the net to the copyright owner.

Finally and perhaps most radically, a world of fast, cheap communication greatly facilitates decentralized approaches to production. One possible result is to shift substantial amounts of human effort out of the context of hierarchically organized corporations into some mix of marketplace coordination of individuals or small firms and the sort of voluntary cooperation, without explicit markets, of which open source software development is a recent and striking example.

### Crime, Cops, and Computers

Some technologies make the job of law enforcement harder. Others make it easier – even too easy. A few years ago, when the digital wiretap bill was going through Congress, critics pointed out that the capacity the FBI was demanding the phone companies provide them added up to the ability to tap more than a million telephones – simultaneously.

We still do not know if they intend to do it, but it is becoming increasingly clear that if they want to, they can. The major cost of a wiretap is labor. As software designed to let people dictate to their computers gets better, that someone can be a computer converting conversation to text, searching the text for keywords or phrases, and reporting the occasional hit to a human being. Computers work cheap.

In addition to providing police new tools for enforcing the law, computers raise numerous problems for both defining and preventing crimes. Consider the question of how the law should classify a "computer break-in" – which consists, not of anyone actually breaking into anything, but of one computer sending messages to another and getting messages in reply. Or consider the potential for applying the classical salami technique – stealing a very small amount of money from each of a very large number of people – in a world where tens of millions of people linked to the Internet have software on their computers designed to pay bills online.

### Designer Kids, Long Life, and Corpsicles

The technologies in our next cluster are biological. Two – paternity testing and in vitro fertilization – have already abolished several of the facts on which the past 1,000 years of family law are based. It is no longer only a wise child who knows his own father – any child can, given access to tissue

samples and a decent lab. And it is no longer the case that the woman from whose body an infant is born is necessarily its mother. The law has begun to adjust. One interesting question that remains is to what degree we will restructure our mating patterns to take advantage of changes in the technology of producing babies.

A little further into the future are technologies to give us control over our children's genetic heritage. My favorite is the libertarian eugenics sketched decades ago by science fiction author Robert Heinlein – technologies that permit each couple to choose, from among the children they might have, which ones they do have, selecting the egg that does not carry the mother's tendency to nearsightedness to combine with the sperm that does not carry the father's heritage of a bad heart. Run that process through five or ten generations with a fair fraction of the population participating and you get a substantial change in the human gene pool. Alternatively, if we learn enough to do cut-and-paste genetic engineering, parents can forget about the wait and do the whole job in one generation.

Skip next from the beginning of life to the end. Given the rate of progress in biological knowledge over the past century, there is no reason to assume that the problem of aging will remain insoluble. Because the payoff not only is enormously large but goes most immediately to the currently old, some of whom are also rich and powerful, if it can be solved it is likely that it will be.

In one sense it already has been. There are currently more than 100 people whose bodies are not growing older because they are frozen, held at the temperature of liquid nitrogen. All are legally dead. But their hope in arranging their current status was that it would not be permanent, that with sufficient medical progress it will someday be possible to revive them. If it begins to look as though they are going to win their bet we will have to think seriously about adapting laws and institutions to a world where there is an intermediate state between alive and dead and quite a lot of people are in it.

## The Real Science Fiction

Finally, we come to three technologies whose effects, if they occur, are sufficiently extreme that all bets are off, with both the extinction and the

radical alteration of our species real possibilities within the life span of most of the people reading this book.

One such technology is nanotechnology – the ability to engineer objects at the atomic scale, to build machines whose parts are single atoms. That is the way living things are engineered: A DNA strand or an enzyme is a molecular machine. If we get good enough at working with very small objects to do it ourselves, possibilities range from microscopic cell repair machines that go through a human body fixing everything that is wrong to microscopic self-replicating creatures dedicated to turning the entire world into copies of themselves – known in nanocircles as the "gray goo" scenario.

Artificial intelligence might beat nanotech in the annihilation stakes – or in making heaven on earth. Raymond Kurzweil, a well-informed computer insider, estimates that in about thirty years there will be programmed computers with human-level intelligence. At first glance this suggests a world of science fiction robots – if we are lucky, obeying us and doing the dirty work. But if in thirty years computers are as smart as we are and if current rates of improvement – for computers but not for humans – continue, that means that in forty years we will be sharing the planet with beings at least as much smarter than we are as we are smarter than chimpanzees. Kurzweil's solution is for us to get smarter too – to learn to do part of our thinking in silicon. That could give us a very strange world – populated by humans, human/machine combinations, machines programmed with the contents of a human mind that think they are that human, machines that have evolved their own intelligence, and much else.

The final technology is virtual reality (VR). Present versions use the brute-force approach: feed images through goggles and headphones to eyes and ears. But if we can crack the dreaming problem, figure out how our nervous system encodes the data that reach our minds as sensory perceptions, goggles and headphones will no longer be necessary. Plug a cable into a socket at the back of your neck for full sense perception of a reality observed by mechanical sensors, generated by a computer, or recorded from another brain.

The immediate payoff is that the blind will see – through video cameras – and the deaf hear. The longer run consequence may be a world where most of the important stuff consists of signals moving from one

brain to another over a network, with physical acts by physical bodies playing only a minor role. To visit a friend in England there is no need to move either his body or mine – being there is as easy as dialing the phone. That is one of many reasons why I do not expect gasoline-powered automobiles to play a major role in transportation a century from now.

A few pages back we were considering a world where realspace was entirely public, cyberspace entirely private. As things currently are, that would be a very public world, since most of us live most of our lives in realspace. But if deep VR gives us a world where all the interesting stuff happens in cyberspace and realspace activity consists of little more than keeping our bodies alive, it could be a very private world.

Having labeled the section science fiction, I could not resist adding a chapter on ways in which current and near future technologies may make possible the old science fiction dream: space travel, space habitats, and perhaps, in time, the stars.

## Alternatives

Any of the futures I have just sketched might happen, but not all. If nanotech turns the world into gray goo in 2030, it will also turn into gray goo the computers on which artificial super intelligences would have been developed in 2040. If nanotech bogs down and AI does not, the programmed computers that rule the world of 2040 may be more interested in their own views of how the human species should evolve than in our view of what sort of children we want to have. And, closer to home, if strong private encryption is built into our communication systems, with the encryption and decryption under the control not of the network but of the individuals communicating with each other – the National Security Agency's nightmare for the past twenty years or so – it won't matter how many telephone lines the FBI can tap.

That is one reason this book is not prophecy. I expect parts of what I describe to happen but I do not know which parts. My purpose is not to predict which future we will get but to use possible futures to think about how technological change will affect us and how we can and should change our lives and institutions to adapt to it.

That is also one reason that, with a few exceptions, I have limited my discussion of the future to the next thirty years or so. That is roughly the point at which both AI and nanotech begin to matter. It is also long enough to permit technologies that have not yet attracted my attention to start to play an important role. Beyond that my crystal ball, badly blurred at best, becomes useless; the further future dissolves into mist.