Oops - We Didn't Mean to Do *That!* -- How Unintended Consequences Can Hijack Good Privacy and Security Policies

Thomas P. Keenan

Faculty of Environmental Design and
Department of Computer Science
University of Calgary
keenan@ucalgary.ca

Abstract. All privacy laws, security policies, and even individual actions are subject to an often-forgotten factor – the "Law of Unintended Consequences" (LUC.) Yet LUC is not a "law" in the sense of appearing in the Criminal Code, nor is it a Law of Nature like gravity. It is actually a manifestation of our inadequate efforts at foresight, and there are things we can do to counteract it. This paper identifies classes of factors which have lead to unintended consequences in the privacy and computer security domains, though the list is by no means exhaustive. It is primarily intended to inspire further thinking and research. We clearly need to make a stronger effort to "foresee the unforeseeable" or at least "expect the unexpected" to maintain public confidence in technological systems. The disciplines of strategic foresight and automated policy analysis may prove useful in attaining this goal.

Keywords: Unintended consequences, technology policy, privacy, security, hacking, strategic foresight, policy analysis.

1 Introduction: The Unintended Consequences Problem

Consider these fictitious news headlines, which are based on real-life cases:

- Canada's Levy on Blank Media Triggers Surge in Cross-Border Shopping
- US Patient Privacy Law Makes it Impossible for Hospitals to Defend Themselves
- Web Browser Flaw Allows Sneaky People to Guess Your Identity
- New Gambling Law Allows Americans to Be Cheated
- Friendly Credit Card Company Sends Barack Obama Card to Someone Else

Each of these cases demonstrates one or more class of unintended consequences. Some are technical, like the web browser exploit; others are corporate and government policy decisions that were not thoroughly considered.

There is a rich body of theoretical literature on the LUC as it applies to technology, much of it from an engineering perspective. Healy discusses unanticipated

S. Fischer-Hübner et al. (Eds.): Privacy and Identity 2010, IFIP AICT 352, pp. 108–119, 2011.

consequences, i.e. "consequences which are not foreseen and dealt with in advance of their appearance." [1] He cautions us not to confuse unanticipated consequences with undesirable or improbable ones. In an example about a nuclear power plant near an ocean, he notes that "the anticipated and intended goal or consequence is the production of electric power. The undesired but common and expected consequence is the heating of the ocean water near the plant. An undesired and improbable consequence would be a major explosion…" Examples from Chernobyl to Three Mile Island tell us that the improbable consequences should indeed be considered in a risk analysis of such a project.

In a book on this subject [2] Perrow also discusses LUC at nuclear power plants, noting that "typical precautions, by adding to complexity may help create new categories of accidents." So, ironically, "at Chernobyl tests of a new safety system helped produce the meltdown and the subsequent fire."

This type of occurrence is what Tenner calls a "revenge effect." In his book on the subject [3] he uses the example of car alarms which are intended to protect vehicles from theft and vandalism. Of course they sometimes malfunction, triggering annoying false alarms with flashing lights and blaring horns. "In cities where alarms are most needed," Tenner writes, "neighbors silence malfunctioning systems by trashing cars." In other words, the technology intended to prevent car vandalism can lead to precisely that.

In the updated edition of his book on highly improbable events, Taleb [4] develops the concept of Black Swans, asserting that all really important discoveries and advances (e.g. the Internet) have come from events that eluded the normal prognostication techniques. So, he writes, "Black Swans being unpredictable, we need to adjust to their existence (rather than naively trying to predict them). There are so many things that we can do if we focus on antiknowledge, or what we do not know."

Dörner [5] provides a helpful framework for understanding why outcomes are often difficult and sometimes impossible to foresee. He notes that complexity, (system) dynamics, intransparence, ignorance and mistaken hypotheses can all play a role in preventing us from correctly foreseeing consequences. A system may simply be too complex or opaque for us to really understand it; it may be changing on its own; or we may simply have inaccurate mental models of reality which make our predictions incorrect.

It is clear that anticipating consequences is hard work, and, sometimes even impossible. Yet it is important work, because we are seeing more and more examples of negative outcomes of bad design at both the technical and policy levels. Without falling into the logical trap of trying to predict what is truly unpredictable, it does appear that there are some common factors that lead to unintended consequences in the domains of privacy, identity and security. It also seems to be helpful to draw on concepts from other disciplines to better understand these issues.

2 Factors That Can Lead to Unintended Consequences

One tool for understanding a complex phenomenon is to identify classes of factors which tend to contribute to it. A related technique is to reason by analogy with other concepts in other fields of human endeavor. The factors listed below, while certainly not an exhaustive list, are intended to shed some light on this type of analysis and to inspire further thinking. They draw on fields as diverse as accounting, information

science, economics, and even human psychology to generate models that can be helpful in this research.

2.1 Materiality – Does This Matter to Me?

In accounting, a sum of money is considered "material" if it could, by its omission or mis-statement, cause the reader of financial statements to form incorrect conclusions about the financial health of the entity. So, a few coins stuck under the cash register drawer are not material, but an unreported commitment to make a large purchase might well be. For the purposes of this paper, policies can be considered material if they have sufficient positive or negative consequences to affect the behavior of a reasonable person.

For example, in the Canadian blank media levy example noted above, the government's stated goal was to collect revenue to compensate musicians for music that was being copied onto blank media. Some argue that reducing media piracy, thereby pleasing the US government, and punishing the Canadian public for audacious copying were secondary goals. There appears to have been no serious contemplation of cross-border shopping in the legislative debate that led to the 1997 changes to Canada's *Copyright Act*. After the fact, the Retail Council of Canada did indeed note the damage to Canadian retailers and is now calling for the abolition of the blank media levy [6]. A similar levy in Australia was struck down by their Supreme Court. Some European countries have blank media levies, as permitted under the EU Copyright Directive of 2001 [7].

Canada's blank media levy is currently 29 cents Canadian per unit for recordable media such as CD-R, CD-RW, MiniDisc, etc. This money is placed into a fund to compensate copyright owners for their losses due to private copying of digital media such as music CDs.

The levy often exceeds the purchase price of the blank CD. Comparing US and Canadian vendors for blank Memorex CD-Rs, a US firm, Best Buy, offers a 50 CD spindle for $16.99 US. The Canadian branch of the same store sells a comparable 50 pack for $39.99. These are regular prices, not temporary sale ones. Since the currencies are currently close to par, the difference in unit price (34 cents vs. 80 cents) is largely due to the blank media levy. Because most Canadians live close to the US border, the temptation to cross-border shop is high and the risk of getting caught is very low. So consumer behavior has changed and the blank media levy is indeed material, in a way that it would not be if it were set at, say, two cents per unit.

2.2 Technology Substitution – Is There Another Way to Do This?

Consumers usually have choices, and will take their business to the vendor who gives them what they perceive as the best deal. For example, many drivers will avoid toll roads, seeking toll-free alternatives, unless the perceived value in terms of time and fuel savings exceeds the toll cost. In a similar fashion, Canadian consumers have "voted with their pocketbooks" by largely shunning the overpriced CDs in favor of other ways of storing digital content. In fact, it is difficult to find blank CDs in many general retail stores. Where did that business go?

DVDs are not subject to the Canadian blank media levy, illustrating the fact that legislation almost always lags behind technology. A spindle of 50 DVD-Rs is available in Canada for $9.99, pushing the unit cost down to 20 cents each, and that's for media with almost six times the capacity of a CD! While it may be annoying to store your music on a disc that will not play in your car's CD player, people are coping by simply transferring their files from DVD to their mp3 player, or even directly to the mp3 player, thereby finding a way around the artificially high cost of CDs in Canada. The advent of cheap flash memory has altered the landscape here, with the very real possibility of storing significant amounts of content in semi-permanent solid state memory.

Of course, this has led the recording industry (the main force behind the blank media tax) to demand a new "iPod tax" to recoup their perceived losses and there is some legislative support for this [8]. This illustrates the iterative nature of policy in which a cycle (some would say an endless and futile one) of measures are proposed, each trying to "plug the leak" discovered in the previous "solution."

The ability to substitute a functionally equivalent technology is certainly an important consideration is searching for unintended consequences, especially in the information technology domain where "a bit is a bit."

2.3 Scope Conflict – My Law Is Better Than Your Law

An interesting situation arose after the passage of the US Health Insurance Portability and Accountability Act of 1996 (HIPPA.) It illustrates a problem when laws (or policies) are created in a vacuum, without paying proper attention to the other laws and policies that will be affected. HIPPA provides much-needed safeguards to give patients control over the use and disclosure of their medical information. However, as a US Federal law, it takes precedence over state laws including the ones that govern lawsuits brought by patients against health care providers [9]. Since the definition of a health care provider in HIPPA is very broad, the net effect of its passage was to allow patients to sue their health care provider and also demand that their information be withheld from the opposing side. The lawyers for the health care providers were thereby denied access to the very information they required to properly build their cases. For a period of time, this caused difficulty in the legal process and had to be addressed by further legislative changes [10].

In a similar fashion, online gambling is currently illegal in the United States by virtue of the enactment of the Unlawful Internet Gambling Enforcement Act (UIGEA) in 2006. Banks and credit card issuers are banned from paying money to online gambling sites. Despite this, offshore online casinos are thriving, and have created an indirect technique called e-wallets to take money from U.S. gamblers. However, if a gambling site fails to pay a winning gambler, there is no way to sue the operators under US law since this activity is explicitly illegal under UIGEA. As Vogel points out [11], if a person wanted to track down their winnings at an offshore casino, "the winner could go to the UK, Aruba or Bermuda, or to the locale stated in the terms of service. It may sound romantic, but it could cost more than it's worth to make the trip -- not to mention payment of litigation fees." Effectively, US-based gamblers using foreign gaming sites are dependent on the honesty and integrity of the site operators as they lack legal protection under the laws of their own country.

2.4 Combinations of Information – The Devil Is in the (Very Minor) Details

Increasingly, the concept of a stateless, memoryless interaction between computers on the Internet is being replaced by a complex and somewhat opaque web of identifications and quasi-identifications. Websites leave cookies, collect personal data, and services like Spokeo (www.spokeo.com) provide easy cross-correlation based on something as simple as an email address. The new web standard, HTML 5, will increase the number of places where cookies can be stored to make them even more persistent and harder to eradicate. Even apparently innocuous leftovers on your computer like the bits that govern what color a link is displayed in can provide clues as to where you've been online. This information is made available to websites via the a: visited pseudo-class, part of the CSS style sheet language that controls how text is presented.

Gilbert Wondracek and Thorsten Holz of the International Secure System Lab at the Technical University of Vienna demonstrated a way to steal the history of a user by exploiting the information that browsers use to render sites that have been previously visited in a different color than other sites [12, 13]. They then combine this with social network sites visited, on the theory that very few people belong to exactly the same combination of social networks. Another researcher, Joerg Resch of analyst company Kuppinger Cole used this technique to uniquely identify himself on the social network Xing and has provided an online experiment to allow others to try to do this [14]. Because of a fix applied to Xing, this technique is no longer functional, but it certainly made a point. One might also argue that if a small set of social networks become dominant, this type of uniqueness will decrease. However, there will always be some class of sites visited that is fairly unique to a specific user and could potentially be exploited.

In a similar spirit, Peter Eckersley of the Electronic Frontier Foundation (EFF) has developed this concept using the precise versions of software installed on a computer (browser, Flash version, plugins etc.) to create a "browser fingerprint." All of the information necessary to create this fingerprint is available upon request to websites visited from the browser [15]. He ran a fingerprinting algorithm on 470,161 informed participants visiting a particular EFF website. Eckersley concluded that, for this sample, "the distribution of our fingerprint contains at least 18.1 bits of entropy, meaning that if we pick a browser at random, at best we expect that only one in 286,777 other browsers will share its fingerprint." He concludes that "there are implications both for privacy policy and technical design." With an estimated 1.5 billion people using the Internet worldwide, browser fingerprinting may not identify a specific person. However, it can certainly be combined with other information to narrow the search.

Clearly the designers of browsers never intended to allow this type of de-anonymization, which is why information such as full browsing history is not passed to websites. However, they failed to realize that through the style information and the a: visited list they were essentially giving out a similar capability to anyone who was clever and devious enough to use it.

It is important to note that combinations of unintended consequence factors may come into play in a specific situation. For example, in the browser exploit example, materiality is also relevant since it would only be worthwhile to bother tracking a user

if there was a purpose, such as sending targeted advertising or something more nefarious, like identity theft or blackmail.

2.5 Pricing Failure – What Is the Price of a Human Life?

It is a basic tenet of economics that "everything has a cost, everything has a price." Yet, the actual implementation of that principle is often flawed. As Schumacher points out "to press non-economic values into the framework of the economic calculus, economists use the method of cost/benefit analysis…it is a procedure by which the higher is reduced to the level of the lower and the priceless is given a price. It can therefore never serve to clarify the situation and lead to an enlightened decision. All it can do is lead to self-deception or the deception of others; all one has to do to obtain the desired results is to impute suitable values to the immeasurable costs and benefits. The logical absurdity, however, is not the greatest fault of the undertaking: what is worse, and destructive of civilisation, is the pretence that everything has a price or, in other words, that money is the highest of all values." [16].

The 2010 oil spill off the US Gulf Coast is a stark example of the difficult of mixing monetary values (getting oil efficiently) with non-monetary ones. Long term ecological damage, injury to British Petroleum's reputation, and loss of human life clearly have symbolic and absolute values that defy translation into dollars and cents. While many observers argue that the spill was predictable, and perhaps even inevitable, few high level decision makers had considered the consequences such as possible health effects from the dispersants being used, as well as the psychological trauma on area residents.

In the realm of privacy and security policies, a dollar cost is often attributed to the compromise of private information, either by citing the amount spent by the party committing the breach to "remedy" it, (e.g. through paying for customers' credit insurance,) or the cost (in time and out of pocket expense) to the victim to reestablish their identity credentials. As one example, TJX Companies, Inc., the US-based parent of retail stores such as TJ Maxx and Winners, estimated the cost of its 18-month long privacy breach at $17 million US [17].

This line of thinking makes the implicit assumption that a victim can be "made whole" by financial compensation. Disturbing examples are arising that demonstrate that is not always possible. According to the media reports, a 24 year old teacher named Emma Jones committed suicide in February 2010 "'after (her) ex-boyfriend posted naked pictures of her on Facebook" [18]. While the man involved denies this action, relatives and acquaintances have stuck to the story that her embarrassment, combined with the fact that she feared legal action as she was living in Abu Dhabi, drove her to take her life. Clearly, for Jones and her family, this privacy breach falls into the realm of "priceless."

Further confirmation that some things are considered "beyond price" comes from the outcry over online tributes to UK gunman Raoul Moat, who attacked a police officer. A Member of the UK Parliament called for the page to be taken down and "took the step of ordering Downing Street officials to contact Facebook, which has allowed 30,000 people to join a bizarre 'tribute group' glorifying Moat's crimes, to lodge a formal protest" [19]. In cases like this, financial compensation seems, as Schumacher argues, to be at best irrelevant and even crass.

2.6 Malicious and Semi-malicious Actors – An Unlocked Door Invites Intruders

No discussion of unintended consequences would be complete without acknowledging the important role of human beings in the ultimate outcome. The term "hacking" has come to refer to the malicious and often criminal activity of breaking into computer systems. However, in its original sense, hacking was a noble calling that saw highly talented people, often at universities, exploring the corners of technology for the sheer joy of it. Levy documented this very well 25 years ago and his book on the subject has recently been updated and re-released [20]. Proof that this playfulness is still with us comes from the case of prankster/journalist John Hargrave [21] who successfully obtained a credit card in the name "Barack Obama" simply by phoning American Express and asking for a "supplementary card" in that name. It was duly issued and arrived in the mail.

Another example relates to the way in which airlines alter fare prices, often in the middle of the night. Clever travel agents wrote automated scripts that queried the airline computers on a continuous basis asking for specific fares on behalf of clients. This put such an unexpected load on the airline systems that they had to put limits on the number of queries made by travel agents.

Many jurisdictions have online systems to allow citizens to check their own, and their neighbors' property assessments for tax fairness purposes. Of course, these are often used for totally unrelated purposes (how much is my boss' house worth?) and this was enough of an issue that the City of Calgary had to take both legal and technical countermeasures to control it [22]. While most people who mis-used this system were, at best, "semi-malicious" in that they were driven by curiosity, at least one person objected when a newspaper published a photograph of his house as one of the most expensive in the city, citing privacy concerns and fears that he would be burglarized.

The best policy in terms of human behavior is to simply assume that if a feature exists in a system, someone will try to figure out a way to exploit it, and will often succeed.

2.7 Future Technologies – Expect the Unexpected

Well beyond the scope of this paper, but impossible to ignore, is the ongoing impact of "not yet invented" future technologies. As one example, petabytes of data are being self-generated by users on Facebook, MySpace, Twitter, etc. and, we can assume, being archived somewhere. Many people even go to the trouble of identifying faces on Facebook through "tagging." Then of course there is the growing presence of surveillance cameras, biometric identifications, etc. Improved facial recognition and data-matching technologies, already under development, will mean that a curious (or malicious) person (or government) in the future may well be able to retrospectively track our movements and perhaps, even, accuse us of committing crimes that aren't even crimes yet!

Sitting between current reality and things not yet invented, there is a whole class of technologies that are already existing, or known to be possible, but which have not yet emerged on a mass commercial basis. Some can be discovered by looking at the patent filings of high tech companies. For example, Apple was assigned a broad patent US

patent 7814163 issued Oct. 12, 2010 [23] under the title "Text-based communication control for personal communication device." It provides an automated mechanism for controlling objectionable language in text messages, and also enforcing certain educational goals. As noted in the patent document, "These embodiments might, for example, require that a certain number of Spanish words per day be included in e-mails for a child learning Spanish." Pundits are already speculating that teenagers will find new euphemisms for the dirty words that are banned, and that pre-written Spanish emails will be readily downloadable to meet the quota requirements.

Those introducing new technologies, whether they are technology providers, network operators, companies, or governments would be well advised to stop and think about possible misuse before releasing new capabilities into the world. Simply stating that "we didn't think of that" will become less acceptable as disgruntled users demand compensation like that exacted from TJX and other firms that have breached consumer privacy.

3 Some Techniques for Anticipating Consequences

Whole organizations have been created to deal with the field of "strategic foresight," an attempt to gain insight into the future without making the assumption that it can be predicted by extrapolation of current situations. While still bedeviled by Taleb's Black Swans, which seemingly come out of nowhere, they have provided useful insights for many organizations. Then again, William Gibson, author of numerous science fictions novels and the man who coined the phrase "cyberspace," has acknowledged "most futurists are charlatans…when I made up that word (in 1982) I had no idea what it meant but it seems to have stuck." [24]

A specific technique within strategic foresight is the use of "scenario planning." Indeed this is the basis of a popular executive seminar taught at many business schools. The one taught at the University of Oxford holds out the promise of "using the future to improve our understanding of today" [25] and traces scenario planning back to the ancient Greeks.

Since scenarios are, in essence, stories about the future, it may well be productive for those faced with privacy and security decisions to adapt sagas like those identified here (and the future will provide a continuous supply.) To illustrate this, consider the case, investigated by the author, of a large US University that compromised the personal data on a large group of students. It happened because a student employee, wanting to test out cloud computing based file storage, needed a large file. He thoughtlessly chose a file containing personal data on all students currently living in the University's residence halls, and posted it on what turned out to be a publicly accessible server at Google. The unencrypted file contained the names, addresses, and social security numbers of a large number of students who had trusted the University to keep them confidential.

The case was further complicated by the fact that the person responsible was a casual student employee and had left the job by the time the matter was discovered. It wound up costing the University a substantial amount of money (to pay for credit insurance for students, etc.) as well as a public relations nightmare that involved writing apologetic letters to affected students.

While the perpetrator's superiors could not have anticipated that he would try to do ill-advised cloud computing experiments, system designers should craft systems, especially those used by casual employees, to restrict file access and sharing. As another example, also investigated by the author, a major Canadian hospital suffered breaches in patient confidentiality because a curious part time nurse made queries on patients all over the hospital with no proper controls.

4 Automated Policy Analysis – A Potentially Useful Tool to Minimize Unintended Consequences

Dan Lin et al. of Purdue University and Jorge Lobo of IBM T.J. Watson Research Center have developed a system called "EXAM - a Comprehensive Environment for the Analysis of Access Control Policies" [26]. It handles policies which can be expressed in XACML, a standard access control language that supports reasonably complex rules. They have recently started applying EXAM to privacy policies and are able to provide quantitative measures of the similarities of two privacy policies as well as identifying contradictions between them and flagging areas that are covered by one but not by the other. They have also developed graphical interfaces to display this information.

Damianou et. al. [27] have created a policy analysis tool called PONDER which provides a declarative language for specifying both security and management policies, as well as a hyperbolic tree viewer, a policy compiler and a policy editor. Acknowledging that "the refinement process is not expected to be fully automated," the authors make provisions for interactive editing, and graphical display. In the future, they hope to add animation.

In the specific domain of privacy, Sirin has applied a policy analysis tool called OWL to the US HIPPA legislation, which governs the use of medical information. As noted in a presentation at the APQC conference in Houston [28] doing a deep analysis of policies does indeed turn up "holes in our policy" (in this case a nurse having "read and re-write" access to medical history files). As policies become more complex, tools like this will become even more necessary, and may help to identify contradictions, inconsistencies, and omissions.

While EXAM, PONDER, OWL, and similar approaches provide excellent technical vehicles for exploring policies, they may be of limited use in finding truly novel unanticipated consequences, simply because the "rule-makers" do not even think about them. How, for example, would browser designers have thought to worry about the color coding of already visited websites? Bertino has expressed enthusiasm for broadening the application of EXAM to other situations such as cloud computing policies, and work on that is ongoing [29].

5 Conclusions

Collecting stories about unintended consequences is certainly entertaining and instructive, and there is every indication that an endless supply of them is forthcoming. Indeed, Peter Neumann of SRI has been hard at work documenting the foibles of technology in the Risks Forum [30] since 1985, and that list of techno-human foibles shows no signs of slowing down. The hard, but really important work, is to derive from

these anecdotes some principles that can help technology developers and policy makers to at least minimize the consequences of the LUC on their work.

Applying concepts from other fields (e.g. materiality from accounting) seems to be a useful tool, and worthy of further exploration. Scenario planning also has a place, especially since it forces people to think about unlikely events and sensitizes them to the inherent unpredictability and inaccuracy of the future.

Black Swans come into play too, but mainly as something to be enjoyed (or not) in retrospect. Taleb makes it clear that attempting to predict them is futile, though we often try to convince ourselves when looking back that developments like penicillin and the Internet were actually logical outgrowths of previous events.

Automated policy analysis is another tool that may be useful. However, it is mainly confined to clarifying the underlying logic of policies. EXAM-like approaches may have some utility in finding subtle contradictions in privacy and security policies, but the really big issues will still require human thought and creativity.

Most of the examples in this paper were gleaned from publicly available sources such as newspapers and Internet postings. There are undoubtedly other rich sources of information about unintended consequences such as the files of national and local privacy commissioners, accident reports filed with government agencies, and internal corporate documents. The advent of "whistle blowing sites" such as the now-famous WikiLeaks can also provide a treasure trove of inspiration, especially as diplomatic cables which were intended for a very restricted audience are read and interpreted by a much broader community.

The real challenge is to understand the underlying patterns of thought and action that lead to unintended consequences, and, where possible, anticipate and prepare for them. This paper has identified seven proposed classes of factors driving LUC. These classes were developed by considering real life instances of unintended consequences and seeking similarities. Ideas from other disciplines such as economics, computer science and accounting were incorporated. The naming of the classes was an important part of the exercise, accomplished iteratively in conjunction with the input of participants in the PrimeLife/IFIP Summer School in August, 2010.

Armed with this model, researchers can take further examples of LUC and decide which category, or categories they fall into, what new categories should be defined, and how the existing ones should be refined. It is also worth noting that the focus of these examples was on undesirable unintended consequences. There is certainly a whole universe of unintended but positive "silver linings" to be explored.

As technology becomes more complex, and makes an even larger impact on our lives, it will be increasingly important to track unintended consequences and to learn from them. Unintended consequences will always be with us – they will just get more subtle and harder to predict as we think harder about them. Still, every instance of an undesirable consequence that is anticipated and avoided is a small victory that should improve our interaction with technology.

Acknowledgements

This work was funded in part by a Research and Study Travel Grant from the University of Calgary. The helpful comments of Prime Life project reviewers and other participants at the August 2010 Summer School in Helsingborg, Sweden are also gratefully acknowledged.

References

1. Healy, T.: The Unanticipated Consequences of Technology. articled posted at Santa Clara University website, http://www.scu.edu/ethics/publications/submitted/healy/consequences.html (accessed February 10, 2011)
2. Perrow, C.: Normal Accidents: Living with High Risk Technologies. Princeton University Press, Princeton (1999)
3. Tenner, E.: Why Things Bite Back: Technology and the Revenge of Unintended Consequences. Vintage Books, New York (1996)
4. Taleb, N.: The Black Swan. In: The Impact of the Highly Improbable. Random House, New York (2007)
5. Dörner, D.: The Logic of Failure: Why Things Go Wrong and What We Can Do To Make Them Right. Metropolitan Books, New York (1989) (English Translation, 1996)
6. Retail Council of Canada Submission – On Copyrights, September 11 (2009), http://www.ic.gc.ca/eic/site/008.nsf/eng/02560.html (accessed February 10, 2011)
7. http://eur-lex.europa.eu (accessed February 10, 2011)
8. Flatley, Joseph, L.: Is Canada's iPod Tax Back? posted March 17 (2010), http://www.engadget.com (accessed February 10, 2011)
9. Antognini, Richard, L.: The law of unintended consequences: HIPAA and liability insurers; at first glance, the Privacy Regulations appear to be adverse to insurers and defense counsel, but McCarran-Ferguson and exceptions may save the day. Defense Counsel Journal 69(3), 296–305 (2002)
10. Kapushian, M.: Hungry, Hungry HIPPA: When Privacy Regulations Go Too Far. Fordham Urban Law Journal 31(6), 1483–1506 (2004)
11. Vogel, P.: US Law Against Online Gambling Makes it the Biggest Loser. E-Commerce Times, September 9 (2010), http://www.ecommercetimes.com/rsstory/70775.html?wlc=1287123815 (accessed February 10, 2011)
12. Cameron, K.: More Unintended Consequences of Browser Leakage, http://www.identityblog.com/?p=1088 (accessed February 10, 2011)
13. Wondracek, G., Holz, T., et al.: A Practical Attack to De-Anonymize Social Network Users. Technical Report TR-iSecLab-0110-001, http://www.iseclab.org/papers/sonda-TR.pdf (accessed February 11, 2011)
14. http://www.iseclab.org/people/gilbert/experiment (accessed February 10, 2011)
15. Eckersley, P.: How Unique is Your Web Browser?, https://panopticlick.eff.org/browser-uniqueness.pdf (accessed February 11, 2011)
16. Schumacher, E.F.: Small is Beautiful – Economics as if People Mattered. Harper & Row, New York (1975)
17. Gaudin, S.: TJ Maxx Breach Costs Hit $17 Million, http://www.informationweek.com/news/security/showArticle.jhtml?articleID=199601551 (accessed February 10, 2011)
18. http://www.huffingtonpost.com/2010/02/26/emma-jones-british-teache_n_477337.html (accessed February 10, 2011)

19. http://www.dailymail.co.uk/news/article-1294700/Facebooks-Raoul-Moat-tribute-page-breached-terms-conditions.html#ixzz0v4NoxM50 (accessed February 10, 2010)
20. Levy, S.J.: Hackers: Heroes of the Computer Revolution – 25th Anniversary Edition. O'Reilly, Sebastopol (2010)
21. Metzger, T.: Prank Uses Obama in Attempt to Obtain Centurion Bling, http://blogs.creditcards.com/2008/10/the-amex-centurion-card.php (accessed October 15, 2010)
22. As explained, https://assessmentsearch.calgary.ca (accessed February 10, 2011)
23. US Patent Office, http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=7814163.PN.&OS=PN/7814163&RS=PN/7814163 (accessed February 10, 2011)
24. Gibson, W.: Wordfest speech at the University of Calgary (October 13, 2010)
25. http://www.sbs.ox.ac.uk/execed/strategy/scenarios/Pages/default.aspx (accessed February 10, 2011)
26. Lin, et al.: EXAM – a Comprehensive Environment for the Analysis of Access Control Policies, CERIAS Tech Report 2008-13, http://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2008-13.pdf (accessed February 10, 2011)
27. Damianou, N., et al.: Tools for Domain-Based Management of Distributed Systems. In: IEEE/IFIP Network Operations and Management Symposium (NOMS 2002) Florence, Italy, April 15-19, pp. 213–218 (2002)
28. Siren, E.: Automated Policy Analysis: HIPAA, XACML and OWL, http://weblog.clarkparsia.com/2008/12/10/automated-policy-analysis-hipaa-xacml-and-owl/ (accessed February 10, 2011)
29. Bertino, E.: Private communication, May 7 (2010)
30. http://www.sri.com/risks (accessed February 10, 2011)