In Asia-Pacific Review, 10:2, November 2003, pp. 120-145

Asia-Pacific Review, Vol. 10, No. 2, 2003

Technological Dimensions of Privacy in Asia

J. D. TYGAR

Users in Asian countries (where adoption of broadband Internet technology is more widespread than anywhere else in the world) harbor notions of computer privacy that differ somewhat from those that are prevalent in Europe and the US. The spate of viruses and worms that has laid bare the security inadequacies of Microsoft's operating system and application software has exacted a particularly heavy toll on computer users in Asia. However, as well as posing challenges to privacy, technology also offers new opportunities for increasing privacy. Doug Tygar, computer science professor at the University of California, Berkeley, examines recent advances in security and privacy research, and suggests that the Asian computing environment represents a uniquely suitable test bed for new privacy technologies. He also highlights the increased popularity in Asia of Linux, the open-source operating system—due in part to its stability, but also to the fact that users need not fear hidden "backdoors" that might compromise security.

Privacy, broadband, and society in East Asia

The last year has seen remarkable developments in both privacy and mass access to information in East Asia. First, consider some of the concerns relating to privacy:

- **Japan**: Mass protests occur after government plans for the "Juki Net," the computerization of the *juumin kihon daichou* (resident's basic registry) which contains personal information about all Japanese residents (including information relating to family and lineage).[1]
- **Taiwan**: Wide concern is expressed over the introduction of island-wide smart cards containing health insurance information.[2]
- **Hong Kong**: After protests that included a march by more than 500,000 of the territory's residents, Chief Executive Tung Chee-hwa was forced to drop an "anti-subversion" law which (together with other measures) would have made on-line access to certain types of document illegal.[3]

ISSN 1343–9006 print; 1469–2937 online/03/020120–145
Carfax Publishing, Taylor and Francis Ltd. <http//www.tandf.co.uk/>

DOI:10.1080/1343900032000148075

- **South Korea**: Teachers unions strongly protest the development of a National Education Information System (NEIS) that would collect information about classroom performance across the country.[4]
- **Mainland China**: According to a report from Harvard Law School, China monitors Internet usage over the popular Google search engine, at one point substituting government-approved Chinese search engines for Google, at other points automatically disconnecting users' high-speed broadband connections when unapproved requests are made.[5]

However, this concern about privacy is taking place against the background of rapidly expanding broadband access throughout East Asia.

Even in 2002, East Asian economies dominated the top of the list of the maximum penetration broadband lines, with South Korea, Hong Kong, and Taiwan all showing dramatic deployment of broadband access:[6]

National Economy	Broadband penetration by percent (number of personal broadband lines/population)
South Korea	20.7
Hong Kong	14.6
Canada	11.1
Taiwan	9.3
Iceland	8.4
Belgium	8.1
Sweden	7.8
Denmark	6.7
Austria	6.6
The Netherlands	6.5
US	6.2
Japan	6.0
Singapore	5.5
Finland	5.3
Switzerland	4.6

More pertinently, the rate of increase of broadband penetration is rapidly increasing. In Taiwan, 2.5 million households, 35 percent of the total 6.9 million households on the island, enjoy DSL or cable modem broadband access.[7]

In Japan, 12 megabit/second DSL access is available for less than US$21/month (as opposed to typical $40 to $60/month prices in the United States for 1.5 megabit/second DSL access), and Yahoo and Softbank station attractive young women outside Tokyo subway stops distributing free DSL modems.[8]

In mainland China, DSL deployment reportedly increased from 440,000 lines at the beginning of 2002 to 2,220,000 by the end of the same year.[9]

In Thailand, deployment was limited by problems with the telecommunications provider, TelecomAsia, which was only able to satisfy half of the DSL requests that it received in 2002. By the end of 2003, Telecomm Asia plans to cover 95 percent of the Bangkok metropolitan area.[10]

Similar rapid deployment is taking place in Australia, Hong Kong, India, Indonesia, Malaysia, New Zealand, the Philippines, Singapore, and South Korea, according to Point Topic, a monitor of international broadband deployment.[11]

This increase in access to information creates a tension between protecting privacy and national pushes to monitor citizen activity—often justified by anti-terrorism, state security, or anti-crime pushes. Countries throughout East Asia have a wide variety of approaches to issues of human rights and state control, and these produce a patchwork of different approaches.

However, it would be wrong to suppose that the only threats to personal privacy come from government actions. Indeed, in many ways, private commercial collection of data represents a far more serious threat. For example, a single commercial firm, Acxiom, collects detailed information about individuals throughout the world which can be used for marketing purposes. Acxiom maintains an office in Tokyo.[12] A crude measure of the dangers posed by mass harvesting of personal information is the scourge of spam electronic e-mail, which now blights virtually all computer users.

An equally pernicious threat is posed by a variety of computer intrusions, and in particular, by computer viruses and worms that can harvest information from individual users. (At the time this article was written, the "SoBig.F" virus was widely believed to be harvesting information about individual computer users.[13]) While computer viruses are a worldwide plague, it appears that in Asia is more vulnerable than other areas. Software piracy has often been noted in a number of Asian economies, including mainland China, Taiwan, Malaysia, Thailand, and Indonesia, thus making users less likely to regularly apply updates or to register their software. The SoBig.F virus struck mainland China (with an estimated 92 percent software piracy rate[14]) quite hard according a recent news account:[15]

> "an Internet worm that turns computers into spam machines has infected 30 percent of all e-mail users in China.... More than 20 million users opened and passed along the Sobig.F virus—called the fastest spreading Web worm ever—to domestic and regional networks, Hao Ting, spokeswoman for Beijing Rising Technology Shareholding Co Ltd, told Reuters. 'We haven't seen anything spread so fast,' she said by telephone. 'It could get worse because there's very limited awareness of viruses and preventive measures.' Hao said the 30 percent figure was based on a study of the firm's one million regular customers and queries at its hotline.

> . . . Hao said only about 60 to 70 percent of Internet users, a total of 68 million people in China by the end of June, had installed anti-virus software and only half of them updated regularly enough to protect against mutating viruses. . . . Users who open the malicious messages turn their own computers into spam relay stations, experts have said. An unprotected public e-mail account set up by Rising to track Internet worms was flooded with 5,000 Sobig.F messages in just three hours on Thursday, Hao said. China, which some call a fertile breeding ground for Internet worms because of rampant piracy of anti-virus software, could help spread the virus more quickly to other countries, experts said. South Korean Internet security companies said damages from the Sobig.F virus were expected to be quite serious before the virus self-destructs in early September. 'There was a huge in jump of virus infections this morning,' said Kim Jung-Hee, a marketing executive at Seoul-based firm Coconut Inc."

These tensions are not only internal to individual economies. According to the head of Taiwan's Defense Ministry's Information and Communications Bureau, Lieutenant-General Lin Chin-ching, Taiwan has developed more than 1000 computer viruses to attack mainland China in a potential cyber-war. Similarly, the recent book *Unrestricted Warfare*, by Qiao Liang and Wang Xiaonsui (both officers in mainland China's People's Liberation Army), offers powerful arguments as to why mainland China should develop aggressive cyber-war technology.[16]

Additional concerns are raised by a new and potentially powerful technology: ubiquitous *sensor webs* formed by inexpensive, tiny wireless sensors that have the ability to monitor people in a wide variety of settings. Academic interest in this technology is high. In the United States, the National Science Foundation recently received over six hundred separate research proposals in just one competition (the 2003 NSF Information Technology Research grant competition) for sensor web research, and in East Asia, Keio University (Japan), National Chiao Tung University (Taiwan), and City University of Hong Kong all have major efforts in this area.[17]

However, just as technology threatens privacy, it also offers new opportunities for privacy. This article discusses potential technical developments that, if successful, could create additional privacy.

Until recently, the computer security community was ill-prepared to address questions of privacy. Indeed, privacy was usually treated as the poor step-child of computer security. Although a leading conference in the field is called the *IEEE Symposium on Security and Privacy*, even a casual glance through any recent proceedings will reveal that privacy usually receives little attention—and when it does, it is ancillary to a much larger and more important point about computer security. Other leading conferences, run by major academic computer science organizations fail to mention privacy in their titles at all, and those conferences are no more likely to feature papers on privacy than any other IEEE conference. However, as this article demonstrates, recent developments in privacy research are showing great promise, and privacy is now enjoying a renaissance in terms of interest within the technical and scientific communities.

An Asian notion of privacy?

There is no clear consensus in Asia on a definition of "privacy." Indeed, there is no clear consensus in the United States or European Union on the meaning of "privacy," although law and judicial procedures tend to point in certain directions. Here are some of the definitions that are current[18]:

- **Privacy is a fundamental human right**. This is stated in Article 8 of the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms. This view has attracted some criticism, since many believe that other human rights (such as a right to a fair trial, the right to freedom of religion, the right to be free of torture) appear to be far more important than privacy. Indeed, the casual regard with which people treat their privacy (for example, gladly giving personal details to qualify for discounts at a local store) would seem to argue that most people do not value privacy as a human right.

- **Privacy is a property right**. According to this view, individuals should have the right to sell or transfer private information using principles derived from intellectual property law. This view has attracted wide criticism since "trades" of private information are usually wildly asymmetrical and because no remedy exists if private information is misused—once released, private information cannot be made private again

- **Privacy is in the shadows of government charters**. This was the view taken by the US Supreme Court when it said that "privacy is in the penumbra of the Constitution" in its decision legalizing abortion in the US, *Roe v. Wade*. While this view has recently be re-affirmed by the US Supreme Court decision in *Lawrence and Garners v. Texas*, it remains controversial since critics claim it extracts a notion of privacy that is never actually claimed in the US Constitution.

- **Privacy is subject to regulatory constraints**. This is *de facto* practice in much of the US and Asia. For example, in the US, the Bork bill (passed after details of the videos rented by a nominee for the US Supreme Court were published in a local Washington, DC, newspaper) guarantees very strong protection of video rental records, while other records are freely available for exchange. Similarly, if someone records an event on videotape and the recording includes sound, different laws protect the visual and the audio part of the recording. This view is hard to justify on the grounds of consistency or logic.

- **You have no privacy: get over it!** This celebrated quote is attributed to Sun Microsystems' chief executive Scott McNealy,[19] and while it may reflect the desperation that some may feel over whether they will ever regain control over their privacy, it hardly constitutes positive advice.

- **Spy states are good for you**. This rather surprising view has been advocated by David Brin in his book *The Transparent Society* in which he argues that if the police can monitor all citizens while the citizens monitor the police for abuses, an ideal society might be attained. While this point of view is interesting, it seems to run counter to general views and the public desire for privacy.

In fact, even in the technical community, the notion of privacy varies tremendously. At a recent conference on software security[20] sponsored by Microsoft, Carnegie Mellon University, and the University of Washington, a variety of views were expressed regarding privacy:

- **Privacy is like an access control**. According to this view, privacy is like the property that computer scientists call *confidentiality*. There is a need to specify who has access to private data and accidental disclosure of that data must be prevented.

- **Privacy is like rights management**. According to this view, privacy relates to the release of information to an outside party (in the same way that many advocate *digital rights management* as a means for protecting intellectual property such as video or audio recordings). This use needs to be restricted. That may mean that data should be marked (or, in the argot of computer science, *watermarked*) in a way that allows it to be traced back to its origin and that allows clear understanding of its rights. According to this point of view, systems (such as Microsoft's proposed Palladium architecture) which would enforce such restrictions would provide maximal protection.

- **Privacy is like data mining**. According to this view, private information can be released in statistical summary or in individual parts. The question is whether sensitive information can be inferred from the private information.

- **Privacy is like data escrow**. According to this point of view, information is recorded, and the fact that it is recorded is known, but the details of the information itself are kept secret. Individuals seeking detailed information would need some sort of permission (an "electronic search warrant") to read the detailed information.

The US response: Terrorism Information Awareness

The roles of privacy, technology, and government have recently been thrown into sharp relief by recent experiences in the US. In the wake of the tragic events of 11 September 2001, the United States created a number of new organizations in order to track potential terrorist threats more effectively, including the Terrorist Threat Integration Center, and two new offices in the Defense Advanced Research Project Agency (DARPA): the Information Awareness Office and the Information Exploitation Office.[21] The Information Awareness Office proposed a controversial program which was initially named Total Information Awareness and later renamed Terrorism Information Awareness (which conveniently allowed the abbreviation TIA to be retained).[22] TIA was headed by retired Admiral John Poindexter. Poindexter proved a contentious choice—he was a former national security advisor to President Reagan and was convicted on multiple felony counts of lying to Congress as part of the Iran-Contra scandal (although his convictions were subsequently overturned by a higher court). By mid-August, criticism had of TIA mounted and on 12 August 2003 he resigned from his position.[23] At the time of writing, the future of TIA is uncertain, as the US Senate has voted to discontinue funding for the program. However, it is widely expected that, in joint conference with the House of Representatives (the lower branch of the US Congress), the Senate will restore the program's funding.[24]

TIA includes a program to integrate data sources so as to allow queries of private information that could span multiple sources. This program is called Genisys (the apparent misspelling being deliberate). To illustrate TIA's objectives, Dr Doug Dyer at DARPA used the example of the notorious Japanese Aum Shinrikyo cult:[25]

"In 1995, Aum Shinri Kyo attacked the Tokyo subway system using sarin gas, killing 11 and sending hundreds to the hospital. This attack is a prototypical, perhaps extreme example of predictive precursor events. Prior to the 1995 attack, Aum Shinri Kyo cultists led by Shoko Asahara had tried to buy US and Russian chemical munitions. When that failed, they engaged in a substantial weapons development program aimed at mass effects. They created elaborate development facilities for producing sarin, purchased expensive equipment, and accumulated huge chemical stockpiles. Following several malicious attempts with ineffective agents, they created a test facility in Australia and tested sarin by killing sheep whose remains were later discovered. Noxious chemical leaks were reported by neighbors near their development facility in Japan, but police still made no arrests. Asahara broadcast his intentions clearly via radio. And months before the subway attack, cultists used sarin in an overt attempt to kill three judges in the city of Matsumoto. In this example, just as in the case of 9/11, fragments of information, known by different parties in different organizations, contained a predictive pattern that could have been identified had the information been shared and properly analyzed."

It is anticipated that the types of information that would be collected under TIA would include communication records, financial records, education records, travel records, records of country entry, place or event entry, medical records, veterinary records, transportation records, housing records, critical resource records, and government records. These records could be gathered either from private sources or from governmental sources.[26]

However, perhaps TIA's most revolutionary idea is the notion that technology itself may be used to protect data. DARPA's official report to Congress explains this as follows:

"The Genisys Privacy Protection Program aims to provide *security with privacy* by providing certain critical data to analysts while controlling access to unauthorized information, enforcing laws and policies through software mechanisms, enforcing laws and policies through software mechanisms, and ensuring that any misuse of data can be quickly detected and addressed."[27]

This suggestion—that technology itself may hold the answer to privacy issues—raises the fundamental issue addressed in this paper. Two classes of this type of protection are particularly worthy of discussion:

- Protection mechanisms imposed by the operators of data aggregation systems
- Protection mechanisms imposed by the subject of those monitoring systems.

The latter class of protection mechanism is particularly interesting, since it raises the prospect of individuals being able to use technology to protect their own privacy in the face of governments, commercial firms, and rogue organizations that threaten to harvest information.

An agenda for privacy research

Here are three techniques that appear particularly promising for privacy protection:[28]

Selective revelation: In aggregate data systems, rather than revealing all data to queries, data can be distributed in discrete chunks that require positive approval to advance. The goal is to minimize revelation of personal data while supporting analysis. This approach revolves around partial, incremental revelation of personal data. Initial revelation is handled by statistics and categories; subsequent revelations occur as justified by earlier results. Such a system is powerful, since it can support both *standing queries* ("tell me the names of all the foreigners from watch list countries who are enrolled in flight school") as well as specific real-time queries ("tell me where the money involved in Transaction X may have come from"). Selective revelation is a method of minimizing the exposure of individual information while supporting continuous analysis of all data. The problem with this is that much of the data is private information about people, which cannot necessarily be revealed to a person. Even data that is derived via an analysis algorithm may be private, depending on the status of the data from which it was derived, and on the nature of the algorithm.

The idea of selective revelation is that, initially, information is only reveal in a sanitized form—that is, in terms of statistics and categories that do not reveal (directly or indirectly) anyone's private information. If a user sees reason for concern, he or she can follow this up by seeking permission to receive more precise information. This permission would be granted (under appropriate legal and policy guidelines) if the initial information provided sufficient cause to allow the revelation of more information.

For example, a government analyst might issue a query asking whether there is any individual who has recently bought unusual quantities of certain chemicals, and who has also rented a large truck. Rather than revealing the identity of any individual, the algorithm could simply respond "yes" or "no." The analyst might then take that information to a judge or an appropriate body, seeking permission to learn the individual's name or other information about the individual. By revealing information iteratively, the disclosure of private information is prevented—except when revelation is adequately shown to be justified.

Selective revelation works by putting a security barrier between the private data and the analyst and by then controlling what information can flow across that barrier. The user injects a query that uses the private data to determine a result, which is a high-level sanitized description of the query result. That result must not leak any private information.

Selective revelation must accommodate multiple data sources, all of which lie behind the (conceptual) security barrier. Private information is not made available directly, but only through the security barrier.

A key technology challenge is to refine data relationships, so as to enable selective revelation. One way to address this challenge is to develop data ontologies that provide structured and logical ways for users to make appropriate queries.

However, (as the careful reader will already have noted), this creates an architectural problem. It is easiest to think of a protective privacy/security barrier as existing outside a single monolithic repository. However, for the applications listed above, the no single monolithic repository exists. In the type of system necessary to support detailed analysis, information must be collected and aggregated from multiple repositories. In this type of system, there can be no central privacy/security barrier—each repository must have its own barriers, and those barriers must be coordinated to support both the privacy restrictions of the system as a whole and the privacy restrictions of the individual repositories.

Strong audit: Perhaps the strongest protection against abuse of information systems is the use of strong audit mechanisms. It is vital to "watch the watchers." These audit systems must be tamper-evident or tamper-resistant, and (since repositories span different organizations) must themselves span different organizations. If such audit mechanisms exist, substantial advantages will be realized, such as identification of spies. However, these audit systems themselves pose a substantial challenge. Audit data will be voluminous and highly sensitive (certainly, foreign intelligence agents would be very interested to learn the kinds of query that are run through a government's commercial or governmental information systems). How can instances of inappropriate queries be detected? In many ways, this is a recursive instance of the general intelligence data-mining problem, and should probably be considered in conjunction with that problem. This hall of mirrors presents a number of technical challenges, and would benefit from the research community's attention.

Better rule proceeding technologies: Distributed information systems combine data from diverse sources. Their privacy systems must support privacy constraints—both systemic privacy constraints and privacy constraints specific to a particular set of information repositories. (For example, information derived from a foreign source, such as country X's information repositories, may come with specific privacy concerns attached.) Since computers cannot in general understand the underlying representation of private information, it is necessary to label data with information that will allow it to be properly processed, both with respect to privacy constraints and with respect to general constraints. Information varies tremendously in quality as well. For example, substantial anecdotal evidence supports the claim that a significant item of data that appears in commercial credit bureau sources is not always accurate. Information from foreign sources may be tampered with. The degree of scrutiny that is applied in efforts to keep data accurate varies considerably

between different government agencies. All of this poses issues for accurate labeling. Further concerns arise since it is highly likely that even a new information system will build on substantial amounts of (unlabeled or inaccurately labeled) previously existing *legacy data*. Moreover, the problems continue to increase in complexity: what happens when data is combined to produce *derived data*. How should the derived data be labeled? A conservative approach would suggest labeling the derived data with the most conservative labels possible. However, in many cases, this will be inappropriate—derived data is often sanitized and poses less privacy restrictions than the original source data used. On the other hand, in some cases derived data may actually be more sensitive than the original source data.

Data labeling is actually an old idea—it dates back to some of the earliest discussions in the security community. Yet, labeling enjoys at best a checkered reputation: for example, as this author has elsewhere argued, data labeling was a spectacular failure in attempts to define standards such as the US Department of Defense's Trusted Computer Systems Evaluation Criteria (the "Orange Book"). However, there is reason for optimism: when labeling is used to support advisory functions or review functions, considerably better performance would be expected than in the classic mandatory security systems that formed the heart of the higher levels of the Orange Book. Indeed, labeling is undergoing something of a renaissance at present, as demonstrated by its use in a variety of digital rights management systems (DRMs). However, it must be noted that these DRM systems are now widely recognized as having only partial effectiveness.

This poses risks in multiple directions. On the one hand, there is the risk that the current complexity of privacy laws and rules may create loopholes that lead to inappropriate disclosure of information. An example of this is provided by the complexity of US privacy laws, as discussed above, under which the rules that apply to video rentals are different from those for books bought at a bookstore, and different rules apply to video recordings and audio recordings. However, Fran Townsend (former US assistant attorney general and head of the US Justice Department's Office of Intelligence Policy and currently with the US Coast Guard) has argued differently in presentations.[29] She maintains that, in many cases, intelligence analysts and law enforcement personnel miss the opportunity to use essential intelligence information; in their desire to comply with privacy rules, government officials fail to use material that they are legally entitled to use. In other words, the haze of privacy law makes officials go beyond legislative and regulatory privacy restrictions, with the result that the government misses the chance to "connect the dots."[30]

Clearly, there is a significant challenge in helping users of databases (whether employees of companies such as Acxiom, law enforcement officials or intelligence analysts) to appreciate what the real privacy restrictions are. Here is a instance in which technology can help—if a "privacy toolbar" that helps inform users of privacy restrictions can be developed, it may be possible to eliminate mistakes caused by

human misunderstanding of the international privacy laws and various national privacy laws. This is especially applicable to cases in which rules interact. If a privacy restriction is in place preventing disclosure of a system, a privacy toolbar could help explain to users the procedures necessary for accessing data legally.

In the domain of more advanced and speculative research, a system can be envisioned which could simulate different information-handling policies. Such a system would use synthetic data and run queries against them. Comparison of different privacy policies might yield examples that will help illustrate the respective advantages and disadvantages of a variety of privacy policies. This could help inform debate by policymakers as they consider different privacy policies. (This stands in marked contrast to contemporary approaches to privacy policymaking, which is often marked by political rhetoric and vague sociological characterizations.) However, such a simulator faces substantial challenges: the simulator itself must be designed, a way must be found to generate meaningful synthetic data, and ways must be found to verify or validate the accuracy of reports from the simulator. These are all difficult problems, and their solution is far from obvious. This is an example of research which is both "high-risk" (the challenges are real) and "high-pay-off" (even partial solutions could help shed considerable light on policymaking).

However, within the framework outlined here, considerable questions remain. One such question is the problem of adaptation. As people realize that certain data is subject to surveillance or response, they change their behavior. Here is an example familiar to any frequent flier: prior to the terrorist attacks of 11 September 2001, many experienced airline passengers angled to be among the very first in line to board commercial airplanes—in that way, the passengers could stow their carry-on luggage and settle in before the rest of the passengers boarded. In the immediate wake of the 9/11 terrorist attacks, authorities instituted thorough searches of some passengers (and their carry-on luggage) as they boarded flights. While these checks were ostensibly random, in fact the security staff tended to select more people from the first few passengers to board a flight. In response, experienced travelers learned to be the tenth in line. Now these boarding searches have become rare, and traditional "push-and-shove to be first" behavior has returned.

In the same way, information systems designed to identify certain groups of people are likely to result in different behavior from both the people they are intended to track as well as innocent people who, for personal reasons, desire to evade surveillance (a case in point being the "arms race" in the United States between telephone caller-ID systems, those who desire to make anonymous calls, and those who desire to reject anonymous calls). Failure to correctly anticipate this sort of adaptation is likely to lead to unexpected and (often undesirable) results. In the worst case, this pattern of adaptation could lead to widespread evasion of surveillance, followed by a counter-move by analysts who need to dig deeper into private data, leading to a spiral resulting in markedly decreased privacy in practice.

To some degree, simulation (as mentioned above) may help prevent this. In addition, however, it would make sense to attempt large-scale experiments with real users. One way to accomplish this may be to adapt commercial multi-player games (along the lines of *EverQuest* or *Baldur's Gate*) to see how real users (albeit, a highly self-selected group) adapt to specific policies.

Are the three research agenda items discussed above realistic, however? Are they within the range of contemporary research? There is considerable reason for believing so:

- Stuart Haber and W. Stornetta have discussed a powerful system for maintaining tamper-evident ordered records, using relatively simple cryptographic mechanisms.[31] Extensions of their system seem likely to be capable of generating audit trails that are immutable—if they are modified, the modification will be readily detectable. This will lead to *strong audit protection*.

- Dawn Song, Adrian Perrig, and David Wagner have presented powerful techniques that allow information to be searched in data repositories, without the nature of the queries or the results being revealed either to eavesdroppers or to the data repositories themselves. This is shown in the Figure below.[32] (Recent work by the author of this article in collaboration with Joseph Hellerstein and Yaping Li considerably extends this technique to allow database matching with complete security.) This yields the ability to *search on encrypted data* without revealing information about the query itself or the response generated. This work yields a surprising result: that it is possible to build databases that are secure—both in a conventional sense and in a new, stronger, distributed sense. This suggests that a number of extensions may be possible. (a) Government agencies may be able to use data from private organizations, such as Acxiom, without revealing the nature of their inquires or searches to Acxiom. Since private commercial organizations often have appalling security (as exemplified by the recent widely reported "identity theft" of highly sensitive private information from private credit agencies and their clients), the protection of the nature of queries is a central concern for effective government use of private information. (b) To the extent that privacy-handling rules can be expressed in computer readable format, it may be possible to enforce privacy restrictions within the framework of an automated processing system. The study does not seek to imply that this technology is ready to use "off-the-shelf"—it does not fully support the functionality listed above and has efficiency issues. However, the theoretical success of the approach by Song et al. suggests that real progress will be possible on an ideal system that will be efficient and that will support the above goals.

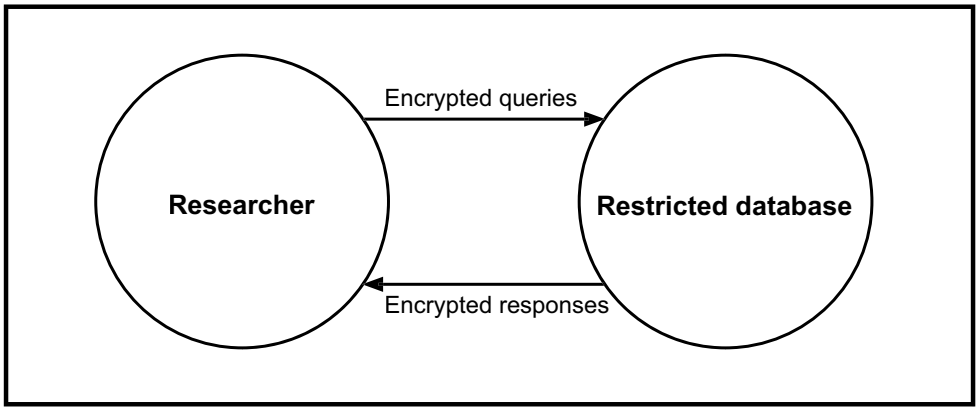

Figure 1. Schematic representation of Song/Perrig/Warner restricted database

- Peter Lee and George Necula have developed proof-carrying code techniques that greatly advance existing abilities to conduct computer *program analysis*.[33] Proof-carrying code allows a computer receiving mobile code to prove that it has certain properties. Further advances lie in the field of static analysis of programs and in projects such as UC Berkeley's Athena system for automatically synthesizing cryptographic protocols with given properties. (Recent work by the author of this article, in collaboration with Li Zhuang, shows how this technique can be used to generate random secure protocols that promise to be highly resistant to contemporary virus and worm attacks.)
- Stunning advances in *dynamic coalitions*[34] have produced research that promises systems that can allow diverse, constantly changing sets of parties to cooperate and work together.

Sensor webs—a future privacy challenge

The preceding discussion on research agendas for privacy focused on mechanisms that protect data aggregation systems. While research challenges still exist in data aggregation systems, these systems (in some form) are already a reality. Japan's Juki Net, Axciom's data services, and South Korea's NEIS are all in existence today. In contrast, sensor webs are an emerging technology that is likely to revolutionize day-to-day life in East Asia.

Sensor webs use small, independent sensors that communicate wirelessly over micro-cells to collect and share a wide variety of information about their environments, including information about people in the environment. As part of the CITRIS project at Berkeley, the author and his colleagues have been developing and deploying such sensors. One of the explicit purposes of such devices is to report on people in a building and the status of the building in the case of a disaster, such as an earthquake, fire, or terrorist attack. These reports are explicitly designed to report on the position and status of people in a building. This raises obvious privacy concerns.

Today, the sensors used are obvious—although they are small, they are still visible to the naked eye. However, with successful further development, some aspire to develop truly dust-sized sensors that could even be mixed in with paint and applied to a wall. Using ambient power sources (such as temperature differentials or small movements), these dust-sized sensors could function indefinitely. By forming an *ad hoc* network on-the-fly, these sensors could pass along a variety of types of information and eventually convey this information to a base station.

Sensor webs are being positioned to make an impact in East Asia that may prove even greater than that of the now ubiquitous cellular phone service. They will provide new ways to monitor, respond to, and influence the behavior of residents. A fictionalized version of a society with sensor web technology was recently depicted in the movie *Minority Report*. In this movie, sensors that use cornea detection are used to identify individuals and provide them with personalized advertisements.

In *Secure Broadcast Authentication*,[35] the author of this paper and Adrian Perrig describe how to arrange sensors into a secure network. The following description paraphrases material from this book which describes the configuration used in an actual system implemented by the authors.

By design, these sensors are inexpensive, low-power devices. As a result, they have limited computational and communication resources. The sensors form a self-organizing wireless network and form a multi-hop routing topology. Typical applications may periodically transmit sensor readings for processing. The current prototype consists of nodes—small battery powered devices that communicate with a more powerful base station, which is in turn connected to an outside network.

At 4 MHz, the sensors are slow and under-powered (the CPU has good support for bit- and byte-level I/O operations, but lacks support for many arithmetic and some logic operations). The processors are only 8-bit devices. (According to figures from DARPA, 80 percent of all microprocessors shipped in 2000 were 4-bit or 8-bit devices.) Communication is slow at a mere 10 kilobits per second.

The operating system for these devices is of particular interest. TinyOS, a small, event-driven operating system, consumes almost half of the 8 Kbytes of the instruction flash memory, leaving just 4500 bytes for security and the application. Significantly more powerful devices would consume significantly more power. Since the devices are powered by a single small battery, they have relatively little computational power. Wireless communication is the most energy-consuming function performed by these devices, so it is important to minimize communications overhead. The limitations of these sensors' power supplies create a security conflict—on one hand, consumption of processor power by security functions needs to be minimized; on the other hand, the limitations of the power supply limits the lifetime of keys (since replacement of the battery is designed to reinitialize the devices and reset the keys.)

Given the severe limitations of such an environment, the technical reader may well doubt that security is even possible. However, in the book, the authors proceed to describe in great detail a set of algorithms which do secure these systems, and further describe an actual implementation of the algorithms on these very sensors.

While security on sensor webs is clearly possible, is privacy compatible with sensor webs? A privacy architecture for a sensor web could be considered at three levels:

Fundamental security primitives: Examples include low-level encryption, authentication, secure broadcast, and synchronization protocols. These constraints make the use of most current secure algorithms impractical.[36] While the challenges discussed here are real, they have already been overcome—for example, in the author's work on the system known as μTESLA.[37] Given the substantial progress in these areas over the past year, this level seems particularly tractable.

Privacy policies:[38] There must be a way to specify exactly what information is recorded, made available and distributed, as well as to whom and under what conditions it is distributed. A large variety of privacy policies are worthy of consideration, for example, "location information of individuals is not recorded or made available except in case of an emergency; and such an emergency must be accompanied by a loud alarm," "users can specify whether they want their location information revealed or not," "location information is made available, but the identities of the persons located are anonymized." In addition to the specification of these policies, a formal, machine-understandable language for interpreting these policies must also be provided.

Human interfaces: Humans interact with sensor webs in at least two ways: as subjects who are potentially under surveillance by the sensor web, and as users who may need to access information collected or synthesized by the sensor web. In both cases, good ways of providing user interfaces are needed. For subjects, there are the questions of how they receive notice ("you are under surveillance in the following ways") and how they specify preferences ("please allow people in my work group to know my location, except when I am on my lunch break."). For users of the sensor web, good ways to specify queries, to receive easily understandable answers to queries, and to specify and monitor policies are all required.

Once these techniques are in place, a variety of important experiments and analyses can be conducted as follows:

Experimentation on Policies: This system can be used to examine the human interfaces so as to determine their clarity and effectiveness, and can also be employed as a sociological test bed for the purpose of gauging the individual's level of comfort with respect to different types of monitoring policies. Do people gradually acclimatize to monitoring policies, or do monitoring policies effect observable changes on behavior and work habits? Is notice effective? Do people understand what is being collected, and what the consequences of this are?

Security Analyses: To what extent are the privacy safeguards that are designed into the sensor web vulnerable to attack? Are there single points of failure which, if breached, present a serious risk of the large-scale release of private information?

Masking Strategies: How effective in practice are anonymizing masking strategies, such as the addition of noise to data or the presentation of data in a purely statistical form?

Legal Analyses: What can be achieved effectively through technology, and what gaps remain? Where is additional regulation required to protect individual privacy? What sort of legal regulation is well supported by technology and what laws are not? Are there laws which are effectively unenforceable because technology cannot support those laws?

A fully completed analysis along these lines could yield a substantially deeper understanding of the privacy issues relating to the use of sensor webs.

Trustworthiness: the relative merits of proprietary software and open-source

In order to make privacy (or any computer function) effective, it must be implemented on a platform that is trusted. This raises an interesting question: since Microsoft, a US company, dominates the market for operating systems, and since large US companies, such as Adobe and Macromedia, dominate software application markets, to what extent can users in Asia trust that their systems are free of backdoors that could allow monitoring of individual users?

This question is not merely a reflection of paranoia. As discussed above, both mainland China and Taiwan are devoting great effort to preparations for military cyber-warfare. It has been speculated (although as yet without foundation) that the US government and the US Defense Department's National Security Agency may have put trapdoors into the Windows operating system.[39] Some Microsoft software has the capacity to monitor detailed operations on a machine. For example, whenever an application crashes, the user is invited to send information about the failed procedure directly to Microsoft. If the user was editing or viewing a document, the information sent would probably allow Microsoft to reconstruct the document. The future looks more ominous. Microsoft has announced a major new initiative (originally code-named "Palladium" and now called the "Next Generation Secure Computing Base") to provide a tamper-proof or tamper-resistant core operating system. This approach has attracted wide criticism, and would enable a variety of schemes for monitoring usage by the end-user and for restricting the function of a machine. (For example, this type of system has been widely touted as a way of keeping content from being transferred from one machine to another.)[40]

Perhaps more significantly, however, software is expensive. A typical configuration with a proprietary operating system (such as Windows XP Professional), an Office Suite (such as Microsoft Office XP Professional), and related software can easily exceed $1000 per machine. (In recent years Microsoft has implemented an activation mechanism that makes it difficult to pirate recent software.) Driven in part by security and privacy concerns, and in part by price concerns, an increasing number of Asian economies are seeing a government focus on the use of alternatives.

A powerful alternative exists. In the last few years, a broad-based "open-source" software movement has been developing an operating system (Linux), office software (OpenOffice), and a variety of applications (including the GNU suite) that generally cost nothing. Some firms, such as Red Hat and SuSe, do charge for physical copies of the operating system, for documentation and for support. However, the same software, and in most cases the same documentation, can be downloaded from the Internet for free. Today, the Linux environment is quite advanced, offering in most cases better functionality, performance, and stability than the Windows operating system. The last major remaining challenge on Linux

platforms is convenient installation, and enormous strides are being made in this direction. More important, the source code (the high-level computer program) for Linux installations and open-source applications is freely available; hence, anyone (such as a national security organization) can inspect it to insure that it contains no backdoors.

Mainland China has taken the lead in promoting the use of open-source software. Red Flag Software distributes a Chinese version of Linux. Red Flag is a state-endorsed effort which enjoys close participation from the prestigious Chinese Academy of Sciences and from China's Ministry of Information Industry.[41] Although maintaining complete control from mainland China, Red Flag is cooperating with a number of firms, including Oracle and the Taiwanese computer manufacturer Acer. In broken English, Red Flag's announcement sounds an echo of previous generations' socialist declarations announcing the unity of workers throughout the world:

> "With regard to cooperation, the CEO of Red Flag indicates that because of the monopolization of source codes and the lack of security of the system, all Windows users have begun to differentiate. On the contrary, Linux has been cooperating with other firms since its establishment, and Linux desktop has won the confidence of prospective customers through its openness, compatibility, individualism, and multi-functionality. When talking about the reasons why customers choose Linux, concerned leaders of Acer said, Linux is powerful in the aspect of desktop as well as in the aspect of server. Openness, steadiness, and individuation of Linux attract customers. We are confident of the development of Linux. The cooperation between Red Flag and Acer is one important step for Linux to gain general recognition."[42]

In response to the rapid growth of Linux in China, Microsoft has released its source code to the Chinese government.[43] Despite this step, however, Microsoft's prospects for long-term success in China remain murky at best.

The rapid growth of Linux is not limited to China. The Taiwanese government has initiated a push to use Linux, so as to avoid an estimated US$59 million in government royalty payments and US$295 million in payments by the private sector.[44] According to a Gartner report study, in 2003 41 percent of firms in the Asia-Pacific region that have more than 500 employees are running Linux (in 2001 the figure was 15 percent). The individual figures for Taiwan and South Korea are 54 percent and 43 percent respectively.[45] In addition, recent news reports indicate that Japan, South Korea, and mainland China intend to embark on a joint effort to develop an open-source operating system that will serve as an alternative to Microsoft Windows. Japan's trade minister, Takeo Hiranuma, indicated that this proposed joint effort was directly motivated by Microsoft's poor record on security.[46]

In Japan, particularly creative versions of Linux abound. Sharp has developed a Linux-based family of "palm computers" (personal digital assistants or PDAs). This family of PDAs, called Zaurus, enjoys an almost cult-like following among computer scientists. In the United States, demand for this product in computer

science departments is so great that researchers are directly importing the product to the US, despite the absence of support for the product in the US, and the absence of an English-language user manual, and completely disregarding the fact that the product is clearly intended for Japanese users.[47]

While it may be premature to declare the victory of open-source software over proprietary software in East Asia, it is clear that open-source is increasing in importance and use. As users and governments regain control of the operating systems and software on computer desktops, they are enjoying both increased possibilities for the development of privacy-enhancing mechanisms and greater freedom from the commercial surveillance that commonly accompanies the use of software products manufactured in the US. However, this same freedom could have other consequences: the lawless reputation of cyberspace is unlikely to be improved by the relative anarchy instigated by open-source software. To counter the specter of this model, enterprises such as mainland China's Red Flag offer a compromise. While still offering independence from foreign interference and fees, Red Flag—with its close government ties—could (in theory) exert a degree of control if the Chinese government felt that users had *too* much freedom. Indeed, the prospects for open-source are far brighter in East Asia than in North America or Europe. While these prospects will have complex consequences, on balance these consequences seem likely to be positive in terms of the protection of individual privacy.

The prognosis for Asia

In many ways East Asia is the ideal laboratory for testing notions of technologically protected privacy. Arguably, Asians enjoy greater access to technology than any other group in the world, with strong technological development in Japan, the dynamism of the Asian tiger economies of South Korea, Hong Kong, Singapore, and Taiwan, and the gradual but inexorable emergence of mainland China. Internet access in a number of Asian economies (including Hong Kong, South Korea, and Taiwan) is approaching ubiquity, and far exceeds levels of Internet access in the United States and most countries in Europe. Japan seems likely to join their exalted ranks within the next two years. East Asia has a wide variety of social and political models, ranging from strong state control to *laissez faire* and to centrally planned growth. Tensions between the East Asian states make the protection of individual computer systems from attack by potentially hostile states a top priority, and both mainland China and Taiwan seem well on the way to developing significant cyber-warfare capabilities.

At the same time, widespread public interest in privacy has made the topic a priority for a large number of Asians. Asia is also refreshingly free from the baggage of dogmatic approaches to privacy. In contrast to the European Union (which has elevated privacy to a human right) and the United States (which seemingly regards privacy as being a distant second to economic development in importance), Asia is free to develop its own approaches to privacy. Now is the perfect time for Asian researchers to assume a dominant role in developing technologies that aggressively seek the limits of the opportunities that technological solutions offer for privacy.

Notes

All Internet references are current as of early September 2003. A missing or dated reference can often be recovered from the Internet Archive <http://www.archive.org/>, even after the original article has been deleted or moved.

1 "There's always someone looking at you—and the people don't like it," *Economist*, 10 August 2002. The system went live on 25 August 2003, ("Juki Net goes into operation," *Daily Yomiuri*, 26 August 2003.)

2 Roger Liu, "Group concerned over new integrated circuit health insurance cards," *Taipei Times*, 15 August 2003.

3 Helen Luk, "Hong Kong eases anti-subversion proposal after massive protests," *Associated Press* story, 28 January 2003; "500,000 take to the streets," *South China Morning Post*, 2 July 2003. Keith Bradsher, "Hong Kong Drops Unpopular Internal-Security Bill," *New York Times*, 5 September 2003.

4 Kim Ji-Ho, "Teachers Threaten Collective Action," *Korea Herald*, 5 May 2003.

5 See Jonathan Zittrain and Benjamin Edelman, *Empirical Analysis of Internet Filtering in China*, 20 March 2003.
See <http://cyber.law.harvard.edu/filtering/china>.

6 This table was compiled by *DigiTimes* using statistics from the International Communications Union (see "Taiwan broadband penetration reaches 35%," *Digitimes*, 18 August 2003).

7 Ibid.

8 Brendan I. Koerner, "Fat Pipe Dream," *Wired Magazine*, August 2003.

9 See <http://www.point-topic.com/scripts/directory/profile.asp?country=40>.

10 See <http://www.point-topic.com/scripts/directory/profile.asp?country=35>.

11 See <http://www.point-topic.com/>.

12 See <http://www.acxiom.com> and Jennifer Barrett, Presentation to Department of Defense Technology and Privacy Advisory Committee, 22 July 2003, available at <http://www.sainc.com/tapac/library/Acxiom%20Testimony.doc>.

13 John Markoff, "Spam-for-Money Plan Suspected by Expert on E-mail Viruses," *New York Times*, 26 August 2003. (Ironically, one of the side-effects of the SoBig.F virus was the temporary shutdown of the e-mail system needed to submit this article for publication.) Spam in general is surveyed in J. D. Tygar, "Spam," *The Encyclopedia of Human-Computer Interaction*, forthcoming. As a measure of the impact of virus spam, at UC Berkeley's Department of Electrical Engineering and Computer Science (EECS), over 200,000 viruses-laden e-mail messages were logged on a single day, 25 August 2003, and on that same day, 340,000 *IP Scans* (to check the vulnerability of individual machines) were detected, of which 80 percent were internal to UC Berkeley. At EECS, of 1500 registered machines, 300 were found to be infected with some virus on that day. (Kim-Mai Cutler, "*Virus, Worm Hit Campus Servers at Record Speed, Research and Data Lost*," *Daily Californian*, 28 August 2003; Huapei Chen, personal communication).

14 Sam Williams, "Profits from Privacy," Salon, 26 September 2002.
See <http://www.salon.com/tech/feature/2002/09/26/piracy_unlimited/>.

15 Juliana Liu, "Survey: Worm Infects 30 Percent Of China E-Mail Users," *Reuters*, 22 August 2003.

16 Francis Markus, "Taiwan's computer virus arsenal," BBC News, 10 January 2000. See <http://news.bbc.co.uk/1/hi/world/asia-pacific/597087.stm>. *Unrestricted Warfare* was published by the PLA Literature and Arts Publishing House in 1999, and an English translation can be found at <http://www.c4i.org/unrestricted.pdf>.

17 Adrian Perrig and J. D. Tygar, *Secure Broadcast Communication in Wired and Wireless Networks*, Kluwer, 2003; also Darlene Fisher, Shieh Shiuh-pyng, Hide Tokuda, Frances Yao, personal communications. Sensor webs are discussed in the section of this paper entitled "Sensor webs—a future privacy challenge." For a fuller discussion of privacy issues in sensor webs, see J. D. Tygar, "The Problem with Privacy," *Proceedings of the Third IEEE Workshop on Internet Applications*, June 2003.

18 This analysis was influenced by a presentation by Pamela Samuelson at the IBM Institute on Privacy on 10 April 2003. Slides of her presentation are available at <http://www.almaden.ibm.com/institute/pdf/2003/PamelaSamuelson.pdf>. See also her article "Privacy as Intellectual Property?" *Stanford Law Review*, 2000.

19 See, for example, Don Tennant, "Q&A: McNealy defends Sun reliability, personal privacy views," *Computerworld*, 27 November 2001.

20 The conference is documented at <http://research.microsoft.com/projects/SWSecInstitute>.

21 US Office of the President, *Fact Sheet: Bush to Create Terrorist Threat Integration Center*, 28 January 2003.
See <http://www.darpa.mil/iao/; http://dtsn.darpa.mil/ixo/>.

22 This paper is not a review of TIA and is not intended either as an endorsement or a criticism of TIA. However, the reality is that commercial firms such Acxiom have substantial data aggregation and surveillance capabilities today. A government system such as TIA is likely—perhaps one that is less ambitious, perhaps one that is more ambitious, or perhaps one that uses different kinds of data. However, it simply defies political imagination to assume that governments will not play a role in using data aggregation techniques that are now ubiquitous in industry. The question raised by this paper is: *Given the contemporary, real development of sensor webs and distributed information systems, what can researchers do to help find ways to protect privacy?*

23 John Markoff, "Poindexter's Still a Technocrat, Still a Lightning Rod," *New York Times*, 20 January 2003; John Poindexter, letter to Anthony Tether, Director of DARPA, 12 August 2003; *Report to Congress Regarding the Terrorism Information Awareness Program*, 20 May 2003.

24 Joshua Partlow, "Senate Votes to Deny Funding to Computer Surveillance Effort," *Washington Post*, July 19, 2003; Dan Caterinicchi, "Defense tries to save TIA," *Federal Computing Week*, 21 July 2003.

25 Doug Dyer, "Genisys," in Department of Defense, *Total Information Awareness*, July 2002. (A CD-ROM containing prepared speeches and presentations prepared for presentation at the DARPATech conference.)

26 J. Poindexter, "DARPA's Initiative on Countering Terrorism: *Total Information Awareness*," July 2002. On the Total Information Awareness CD-ROM, as described in the previous note.

27 *Report to Congress*. The reference to "security with privacy" (italics in original) is an apparent reference to a report, written by a committee chaired by the author of this report: ISAT, *Security with Privacy*, 13 December 2002, available at <http://www.darpa.mil/iao/secpriv.pdf>.

28 This description is modified and abridged from the ISAT study mentioned above. For a fuller exposition, please see the text of the ISAT study, which was written by the author of this article.

29 One is described in "The Problem with Privacy," Proceedings of the Third IEEE Workshop on Internet Applications, June 2003.

30 This was a common criticism of US intelligence agencies after the 9/11 terrorist attacks.

31 S. Haber and W. Stornetta, "How to Timestamp a Digital Document," *Journal of Cryptology*, Vol. 3, No. 2, pp. 99-111, 1991.

32 D. Song, D. Wagner, and A. Perrig. "Practical Techniques for Search on Encrypted Data" in *Proceedings 2000 IEEE Symposium on Security and Privacy*.

33 See <http://raw.cs.berkeley.edu/pcc.html>. See also George C. Necula, "Proof-Carrying Code," Proceedings of the ACM Conference on Principles of Programming Language, January 1997.

34 See <http://www.darpa.mil/ato/programs/dynamiccoal.htm>.

35 Perrig and Tygar, *op. cit.*

36 For example, the working memory of a sensor node is not sufficient to hold even the variables for *asymmetric cryptographic* (that is, public key cryptography) algorithms (for example, RSA with 1024 bits), let alone perform operations with them. A particular challenge is broadcasting authenticating data to the entire sensor web. Current proposals for authenticated broadcast are impractical for sensor webs. Most proposals rely on asymmetric *digital signatures* which can confirm that data was sent as intended by the originator. Digital signatures are impractical for multiple reasons, including long signatures with a high communication overhead of 50 to 1000 bytes per packet and a high additional overhead for creating and verifying the signatures. Researchers have analyzed the computation of various digital signature algorithms on various platforms—the popular *elliptic curve cryptography* signature algorithms require between 1.0 and 2.2 seconds for one signature generation and between 1.8 and 5.3 seconds for verification on a Palm Pilot. On the same architecture, a 512-bit RSA signature requires between 2.4 and 5.7 seconds for generation and between 0.1 and 0.6 seconds for verification. (M. Brown, D. Cheung, D. Hakerson, J. Hernandez, M. Kirkup, and A. Menezes, "PGP in constrained wireless devices," *Proceedings of the 9th USENIX Security Symposium*, August 2000.) In order to understand the significance of these results, it must be remembered that a Palm Pilot is a veritable supercomputer compared to the sensor motes which were being used, and could compute hundreds of timed faster.

37 Perrig and Tygar, *op. cit.*

38 In this instance the term "policy" is intended in its technical sense, to mean "a set of rules," rather than in its more general sense (as an instance of public policy).

39 James Glaves, "Debate Flares over MS 'Spy Key'," *Wired News*, 4 September 1999. See <http://www.wired.com/news/technology/0,1282,21589,00.html>.

40 Robert Lemos, "What's in a name? Not Palladium," CNET News.com, 24 January 2003. See <http://news.com.com/2100-1001-982127.html>.

41 See <http://www.redflag-linux.com/egyhq.html>.

42 News release, "The Red Flag Software Company cooperates with Acer Linux," 29 May 2003.
See <http://www.redflag-linux.com/jujiao/enews_view.php?id=1000000014>.

43 Li Heng, "Microsoft Gives Chinese Government Access to Windows Source Code," *People's Daily* (English-language version), 4 March 2003.

44 Tiffany Kary, "Taiwan opens arms to open source," *CNET News.com*, 5 June 2002. See <http://asia.cnet.com/newstech/systems/0,39001153,39046684,00.htm>.

45 "Taiwan, Aus top Linux list: Gartner," *CNET News.com*, 13 August 2003.
See <http://asia.cnet.com/newstech/systems/0,39001153,39145673,00.htm>.

46 Martin Williams, "Japan, China, Korea plan joint open-source project," *Infoworld*, 4 September 2003. In response to this announcement, Tom Robertson, Microsoft's director for government affairs in Asia, dismissed Microsoft's vulnerability, reportedly saying "Pointing to a particular software vendor and to a particular software [standard] gets you nowhere," ("Microsoft: Asia not playing fair over OS," *Reuters*, 5 September 2003. These events were still unfolding at the time of writing.

47 In UC Berkeley's Computer Science Division, where the author teaches, the most advanced Zaurus PDA, the SL-C760, is the computational platform whose popularity among both faculty and students is growing the most rapidly, despite the fact that a complete configuration (including wireless access and memory card) costs over US$1200.

About the author

Doug Tygar is a professor of computer science and information management at the University of California, Berkeley. His work is concentrated in the fields of computer security, privacy, and electronic commerce. His current research topics include strong privacy protections, security issues in sensor webs, and digital rights management. His newest book, "Secure Broadcast Communication in Wired and Wireless Networks" (with Adrian Perrig), was published in early 2003. He has designed cryptographic postage standards for the US Postal Service and has helped build a number of security and electronic commerce systems, including Strongbox, Dyad, Netbill, and Micro-Tesla. He serves as chair of the Defense Department's ISAT Study Group on Security with Privacy, and is a founding board member of ACM's Special Interest Group on Electronic Commerce. For many years Dr Tygar was tenured faculty at Carnegie Mellon University's Computer Science Department (where he still retains the position of adjunct professor). He was named an Okawa Foundation fellow for 2003-2004 and a US National Science Foundation presidential investigator. He received his doctorate from Harvard and his undergraduate degree from Berkeley.

Author's acknowledgments

The author wishes to thank the National Science Foundation and the US Postal Service for supporting this research in part. The author also benefited from conversations with members of the ISAT Committee on Security with Privacy, Admiral John Poindexter and other members of Information Awareness Office at DARPA, Professors Suchu Xiaoniu Hsu, Adrian Perrig, Pamela Samuelson, Dawn Xiaodong Song, and Paul Wright, Mr Tom Kalil, Ms Deirdre Mulligan, and students in the author's fall 2002 graduate seminar on privacy.

The author's thinking in regard to this paper was stimulated during a visit to Asia. The Tokuda Lab at Keio University, the Institute for International Policy Studies (IIPS), and the National Science Council of Taiwan (through the International Computer Symposium) helped provide partial travel support to present preliminary versions of this material in Japan and Taiwan. The author is particularly grateful to Mr Isao Hiroki, Professor Shieh Shiuh-pyng, and Professor Hide Tokuda for facilitating this Asian support. He would also like to thank Ambassador Yoshio Okawara, president of IIPS, for encouraging this paper and for his valuable comments on an earlier presentation of this work.

While the author benefited from a broad variety of advice, input and financial support for this study, the opinions in the report are his own, and do not necessarily reflect the opinions of any person or organization mentioned above, of any funding agency, of any government, or of any government agency.