Epilogue: The Broader Perspective

> *An idealist believes the short run doesn't count. A cynic believes the long run doesn't matter. A realist believes that what is done or left undone in the short run determines the long run.*
>
> — Sydney J. Harris, quoted in *Reader's Digest*

In this epilogue we discuss a number of alternative approaches towards privacy, and show how they fail. On the basis of this analysis, we argue that privacy-enhancing technologies (such as those developed in this book) complemented by legislative measures provide the best way to protect privacy and guarantee security.

The limitations of privacy legislation

In many countries, particularly in Europe, the prevailing approach to protect privacy is privacy legislation. Legislation can discourage systematical abuse by the private sector, but is insufficient in all other cases:

- The key paradigm of legislation is to make undesired actions a crime and to prosecute them. This hardly deters criminals who commit their crimes using computers: in today's networked environment they can operate over large distances and remain virtually untraceable, making it difficult to enforce laws and to prosecute suspects.

- In an age where organizations can communicate and transact with individuals all over the world through telecommunication infrastructures, global harmonization of privacy laws is imperative. This, however, is a daunting task that may never be accomplished at all due to cultural differences.

- Attempts to stop organizations from using privacy-invading practices that are in conflict with privacy legislation can easily take many years. For example, in August 1998 the U.S. Federal Trade Commission finally succeeded in ordering Trans Union (one of the three largest U.S. credit bureaus) to stop distributing and selling target marketing lists based on consumer-credit data for unauthorized purposes; the original charge that Trans Union's sale of target marketing lists violated the Fair Credit Reporting Act dated back to 1992.

- Privacy laws put the burden upon individuals to protect their own data, but the complexity and diversity of privacy laws makes it almost impossible for individuals to be aware of their privacy rights. Privacy laws encompass international laws, constitutional laws, case law, and federal, state, and local legislation. According to StateNet, the number of privacy bills introduced in U.S. state legislatures exceeded 8500 in 1997 alone.

- The language of privacy legislation is necessarily broad, even when applicable only to a certain industry sector. This makes it difficult to interpret a piece of privacy legislation in the context of a given communication or transaction mechanism. Consequently, it is hard for data collectors and auditors alike to determine whether privacy legislation has been lived up to. To illustrate the point, the definition of personal data by the European Privacy Directive [157] considers anonymous and pseudonymous data to be different from personal data, but it is unclear where to draw the line. Reidenberg and Schwartz [318] study the degrees to which different E.U. countries and institutions view this data different from personal data, and conclude: "For on-line services, the determination of whether particular information relates to an 'identifiable person' is unlikely to be straightforward."

- New technologies develop much faster than law. With each new consumer technology it can take many years to understand its privacy implications and develop adequate new policies. Even seemingly simple issues, such as whether issuers of electronic cash fall within the definition of "financial institutions" of the U.S. Right to Financial Privacy Act of 1978, are hard to decide. As Oleinick [290, Chapter 7] points out, "What this policy lag means for our society is that the Judiciary is always struggling to extrapolate old laws to cover new technologies, that the Legislature is engaged in continual policy analysis of new technologies once the new technology has created a policy issue, and that the Executive is always struggling to mandate effective Federal policy to regulate agency usage of new technologies."

- Laws cannot protect against the theft or modification by hackers of personal data stored in computer databases, nor against misuse by employees and other individuals authorized to access databases. Netsolve Inc. analyzed over half a million security alarms from May to September of 1997, and found that "every

one of its electronic commerce customers suffered at least one serious network attack per month. [...] The attacks stem from external sources seeking to gain root access to a site's network. Once they gain that access, they possibly could download customer lists, change files, access new product information, destroy data or transfer funds from the finance system." Insider abuse accounts for the majority of Internet security incidents reported to the CERT Coordination Center from 1989 to 1995; see Howard [213] for an analysis.

- Requirements to allow individuals to give notice, to request consent, and to correct inaccurate information in their files may be technically impractical for organizations, and may be difficult to carry out while at the same time adequately restricting employee access.

- New laws frequently exempt earlier provisions in law for the purpose of increasing the surveillance power of the government. For instance, the 1996 amendments to the U.S. Fair Credit Reporting Act of 1971 preempt provisions of stronger state credit reporting laws by permitting the subsidiaries of a parent company to share information without the consumer's permission or government regulation; see the Center for Public Integrity [83] for details. More generally, even in democratic societies there is the realistic threat that privacy laws will be amended, changed, exempted, overturned, or simply ignored.

Privacy legislation can actually contribute to degrading privacy. Where individuals at the time of data collection felt protected by privacy laws, they are likely to have been less inhibited in their behavior than they would have been otherwise. The harmful consequences of privacy intrusions in these cases may be more serious than had the individuals not been given the illusion of privacy in the first place. Furthermore, to check compliance with privacy legislation it is unavoidable that regular audits be performed on the databases of organizations; this increases the accessibility of personal data records, which broadens the scope for abuse. For instance, government agencies may abuse privacy laws to gain access to the databases of target organizations.

The ineffectiveness of self-regulation

The approach of privacy through self-regulation, defined by the Federation of European Direct Marketing [166] as regulation imposed by practitioners on practitioners, and heavily promoted by the United States, is even less effective. Marketers and other data miners have major commercial incentives to use personal data in any way they see fit. Large profits can be made by using and selling consumer profiles, and so any sane person would consider it a serious waste of resources to not put personal data that has already been collected to new business uses. Since organizations can rarely be held liable to compensate consumers for damages caused by the misuse of

personal data, not in the least because individuals often have no clue as to the origin of privacy breaches, organizations are incited to stay on the edge of what would invoke immediate regulatory action.

Another problem is that self-regulation requires the participation of the entire industry, but this is an unrealistic goal: new companies may prefer not to comply, companies that agree to guidelines may in fact not comply with them, and there will always be short-term incentives to ignore voluntary privacy measures. As Canada's Task Force on Electronic Commerce [370] points out, this can "undermine fair competition in the marketplace, creating an unlevel playing field. It can also erode consumer confidence in an entire industry and create further confusion about rights and rules."

Also, self-regulation does nothing to protect against the abuse of private-sector and government databases by government officials and agencies. In fact, adopting privacy principles that explicitly state that law enforcement will not be given access to personal data are in violation of the law in most developed countries.

Most of today's self-regulation initiatives provide only the possibility of opt-out; they do not require explicit customer consent to use or distribute personal information. Many organizations are actively lobbying to prevent opt-in from happening. In discussing the amendments to the U.S. Fair Credit Reporting Act, the Acting Comptroller of the Currency [391] said: "I have even heard of people getting two separate notifications covering different types of information, requiring two separate letters to opt out. Such techniques may fall within the letter of the law, but they certainly fall short of its spirit." Furthermore, none of the industry self-regulation initiatives have an adequate enforcement mechanism, a method for consumers to access their own data, or a way of correcting errors that may have occurred in the transcription, transmission, or compilation of their personal information. Rotenberg [327] warns that self-regulation has "made it harder for us to focus on the larger questions of a coherent privacy policy. [...] Where once there was an understanding that individuals should have the right to get access to their own data, to inspect it, and to correct it, now those who favor self-regulation believe it is necessary only to provide access to a privacy policy."

Surveys consistently confirm the ineffectiveness of self-regulation. See, for instance, surveys conducted by or on behalf of the Center for Democracy and Technology [82], the Electronic Privacy Information Center [143, 144], the European Commission [315], the Federal Deposit Insurance Corporation [162], the Federal Trade Commission [165], and OMB Watch [291]. For other critiques, see the American Civil Liberties Union [10], Budnitz [65, 66], Clarke [118], Rotenberg [327, 328], and Varney [381].

Industry privacy violations confirm that self-regulation is just a smoke screen. Here is a small sample of recent privacy violations:

- In 1998, the U.S. Federal Trade Commission found that Web portal Geocities was selling demographic information collected from its millions of customers

(provided when they signed up for free homepages) to advertisers, even though its online assurance pledged that it would not do so. Ironically, Geocities received a privacy label from TRUSTe (an organization that regulates Internet privacy policies for over 500 companies and gives out privacy seals to conforming Web sites) while it was being investigated by the Federal Trade Commission.

- In January 1999, the chief executive officer of Sun Microsystems (a prominent member organization of the U.S. Online Privacy Alliance) called consumer privacy a "red herring," and proclaimed "You have zero privacy anyway. Get over it."

- In March 1999, TRUSTe decided that Microsoft (one of TRUSTe's largest benefactors) would not be audited for its practice of embedding traceable serial numbers (covertly captured by Microsoft when customers registered their Windows 98 software) into all documents created with Word and Excel.

- One month later, the BBBOnLine Privacy Program (similar to that of TRUSTe) rewarded a privacy seal to Equifax (one of the three largest U.S. credit bureaus), which in the years before repeatedly breached basic privacy principles.

- In May 1999, the Federal Trade Commission settled with Liberty Financial Companies; the company's Young Investor Web site falsely represented that personal data collected from children in a survey would be maintained "totally anonymous," yet it stored all the data in an identifiable manner.

- In November 1999, DoubleClick, which serves over 1300 Web sites with target banner advertisements, acquired market researcher Abacus Direct, which collects data from 1100 merchandise catalog companies. DoubleClick's goal was to correlate the shopping and browsing habits of Internet users with their names and addresses, in spite of its Internet privacy policy that promised that all collected data would be anonymous.[12]

- Also in November 1999, it came to light that RealNetworks was surreptitiously gathering data about the listening activities of users of its music software, and that it recorded this data into a central database. TRUSTe did not revoke RealNetworks' privacy seal.

Since its inception in 1996, TRUSTe has investigated hundreds of privacy violations but has not revoked a single privacy seal.

The latest privacy contempt are infomediaries, a business model devised by Hagel and Singer [205]. Startups such as Enonymous, Lumeria, PopularDemand, PrivacyBank, Privada, PrivaSeek, InterOmni, and @YourCommand aim to become one-stop

[12] DoubleClick's stock took a huge hit after the news became public, and the Federal Trade Commission and several states started an investigation. Hereupon, DoubleClick announced to suspend its plans.

brokers of personal data by persuading individuals to funnel all their transactions through their company. The infomediary's sole goal is to earn revenue by selling the personal data of their customers to marketers. The business strategy to lure unwitting individuals into placing all their data and trust in them is to promise them a piece of the revenue and to post a privacy policy.

The fallacy of key escrow

Anyone who considers "key escrow" as a way of protecting privacy is, of course, in a state of sin. On a fundamental level, there can be no mistake about this. Westin's [387] widely accepted definition of privacy (see Section 1.2.1) clearly requires that individuals themselves are in control over their own information. Key escrow (also known under such names as "key recovery," "revocable privacy," "controlled anonymity," or "trustee-based tracing") takes away this control completely, and therefore offers zero privacy. Splitting the ability to recover the secrets of an individual among multiple key escrow authorities (using secret-sharing) does not change this fact, not even if there would be a gazillion authorities that would pledge to notify individuals before reconstructing their secrets.

On a more practical level, all key escrow systems have the following dangers in common:

- As the NSA [279] (of all parties) warned, law enforcement agents and officials operating key escrow centers could well pose the greatest threat to a key escrow encryption system. Clearly, the same objection holds for any other kind of key escrow system. Abelson, Anderson, Bellovin, Benaloh, Blaze, Diffie, Gilmore, Neumann, Rivest, Schiller, and Schneier [2] note that insider abuse "can even become institutionalized within a rogue company or government."

- On a related note, judicial knowledge and consent may easily be circumvented. Epstein [154] warns that any key escrow system "cuts out the notice and knock provisions that must be satisfied before a warrant could be executed. It vests vast powers in third-party agents who have neither the incentive nor knowledge to contest any government intrusion. It presupposes uniform good faith by public officials and overlooks the major costs of even a tiny number of official misdeeds or mistakes." Also, it will be difficult for courts to enforce the time-limits of a warrant.

- The key escrow authorities become a highly visible target to criminals who seek to trace or decrypt the communications and transactions of certain targets. They may be able to obtain the key shares of their interest through bribery, hacking, or extortion.

In the words of Rivest, in his letter of June 1997 to the senators of the Senate Commerce and Judiciary Committees, "Putting key recovery into cryptography is like

soaking your flame-retardant materials in gasoline – you risk a catastrophic failure of the exact sort you were trying to prevent."

Other general objections to key escrow include the following:

- As Directorate-General XIII of the European Commission [137] points out, "if citizens and companies have to fear that their communication and transactions are monitored with the help of key access or similar schemes unduly enlarging the general surveillance possibility of government agencies, they may prefer remaining in the anonymous off-line world and electronic commerce will just not happen."

- Once a key escrow system is in place, the case for weakening the rules under which escrow access may be gained will gradually be weakened. Already, the FBI and law enforcement agencies in other democratic countries are seeking to gain access to personal data records without needing a court order or a search warrant.

- Key escrow systems may not be legitimate. The Office of Technology Assessment, in its 1985 evaluation [284] of the FBI's National Crime Information Center, pointed out that "first amendment rights could be violated to the extent a national computer-based surveillance system was used to monitor the lawful and peaceful activities or associations of citizens or if it were to have the effect of discouraging such activities or associations. Fourth amendment rights could be violated if the surveillance amounted to an unreasonable search and seizure of personal information. And, [...] fifth amendment rights to due process could be violated if such surveillance was conducted without first establishing probable cause or reasonable suspicion and without serving advance notice on the subject individual." Key escrow systems reverse the presumption that individuals are free until they pose a threat of material harm, and are likely to violate all three amendments on the same grounds. See also Sullivan [366].

In recent years, cryptographers have worked fiercely to replace privacy-protecting systems by key escrow systems:

- The first area that fell victim is electronic voting. Following several proposals that guaranteed unconditional privacy, Cohen and Fischer [119] and Benaloh and Yung [26] introduced key escrow electronic voting. Virtually all electronic voting schemes proposed since then are key escrow systems; for recent achievements, see Cramer, Franklin, Schoenmakers, and Yung [124] and Cramer, Gennaro, and Schoenmakers [125].

  Surprisingly, the transition from privacy-protecting electronic voting schemes to key escrow voting schemes has gone by almost unnoticed and unchallenged. This is because key escrow electronic voting was not proposed to enable law enforcement to trace votes, but as a way to achieve the property of "universal

verifiability;" the terminology "key escrow" never entered the electronic voting vocabulary. It is not clear, though, that universal verifiability is such an important property that it is worthwhile to sacrifice privacy, nor has it been proved that privacy and universal verifiability cannot be achieved at the same time.

Another issue worth mentioning in this context is that the key escrow voting schemes that achieve information-theoretical "untraceability" (with respect to other parties than the key escrow authorities) require the voter to encrypt each of his or her votes for each of the key escrow authorities. The more efficient schemes achieve only computational untraceability: anyone who can feasibly solve (an instance of) the underlying hard problem can trace all votes without the involvement of the key escrow authorities. For a discussion of the drawbacks of computational privacy, see Section 1.3.5.

- The approach of key escrow is most widely associated with public key encryption. See Denning and Branstad [132] for a taxonomy of key escrow encryption systems, and Denning [131] for descriptions of 33 proposed key escrow encryption products and proposals. (Many others have been proposed since the latter reference.)

  The security benefit pursued in this case is the ability to wiretap the conversations of criminals in (near) real time. Numerous publications and testimonies, though, convincingly argue that key escrow encryption will cause much more harm than good. See, for instance, Abelson et al. [2], Bowden and Akdeniz [43], Epstein [154], Froomkin [176], Nathan Associates [274], the NSA [279], Shearer and Gutmann [349], the U.S. National Research Council [278], Walsh [386], and a 1998 background report [15] for the Danish Ministry of Research and Information Technology.

- The most recent area that has fallen victim is electronic cash. Starting with Chaum [105], a floodgate of papers on key escrow electronic cash opened: Brickell, Gemmell, and Kravitz [62], Stadler, Piveteau, and Camenisch [360], Camenisch, Maurer, and Stadler [70, 71], Fujisaki and Okamoto [178], Jakobsson and Yung [220, 221, 222], Davida, Frankel, Tsiounis, and Yung [128], Radu, Govaerts, and Vandewalle [317], Frankel, Tsiounis, and Yung [173, 374], Nakayama, Moribatake, Abe, and Fujisaki [272], and many others.

  Here, the primary excuse to squander privacy has been to combat money laundering. However, money laundering concerns can be addressed effectively without giving up privacy by (prudently) applying one or more of the following measures: placing limits on amounts; ensuring payee traceability (by the payer only); limiting off-line transferability; limiting the issuance of electronic cash to regulated institutions; disallowing anonymous accounts; issuing only personalized paying devices; identifying payers in high-value transactions; and,

> checking the identity of parties who convert other forms of money into electronic cash.
>
> Other excuses for key escrow have been to deal with theft or extortion of the bank's secret key, and to deal with attackers with "infinite" computing power. In Section 5.5.5, however, we have seen that these are not valid excuses either to destroy privacy. Also, in Section 6.4.4 we have shown how to combat extortion of the certified key pairs of certificate holders. [13]
>
> Furthermore, the proposed key escrow electronic cash systems that circumvent involvement of the key escrow authorities in the withdrawal protocol achieve only computational "untraceability" (with respect to other parties than the key escrow authorities).[14]

Much of the key escrow work sports exaggerated and even downright ignorant statements about how privacy will hurt individuals, organizations, and societies at large. Some comfort may be derived from the observation that most authors of key escrow papers in all likelihood had little more on their minds than the urge to publish yet another paper. Waving the key escrow magic wand is the quickest way to success whenever more honorable approaches to improve a line of research are unsuccessful. By radically changing the model to key escrow, the researcher all of a sudden finds him or herself in the luxurious position of being able to claim and glorify new security benefits and features. At the same time, the key escrow smoke screen enables the researcher to downplay the annihilation of privacy by claiming that the new system provides "balanced" privacy; many authors do not even shy away from claiming that their key escrow systems "preserve" or even "improve" privacy.

This down-to-earth explanation of why key escrow approach has been running rampant does not make the trend any less disquieting or harmful, though. If nothing else, the key escrow work has resulted in greatly eroded levels of awareness among fresh researchers of the meaning and importance of privacy.

Some proponents of the key escrow approach argue that the assumption of an anonymous channel (over which to send blind signatures, say) is essentially as strong as the assumption that the key escrow authorities will not pool together their key shares, "because" anonymous channels also rely on some kind of threshold assumption. (Indeed, the electronic voting schemes of Chaum [94] and Bos [42, Chapter 3] rely on a "mix" network.) This argument does not hold water, though. In the physical world, covert mass surveillance of identified individuals is completely infeasible;

[13] In another proposal by Pfitzmann and Sadeghi [302], each user plays the role of the key escrow authorities by him or herself. The drawback of this proposal is that payments are only computationally untraceable. On the upside, the proposal works also in software-only settings. The same technique can be used to protect against extortion of certified key pairs in our software-only setting.

[14] Another drawback is that virtually all the proposed key escrow cash systems require payments to be online to guarantee prior restraint of double-spending or do not address any of the privacy issues associated with smartcards (see Chapter 6). The only exception is a system proposed by Camenisch, Maurer, and Stadler [71], which hereto uses techniques developed in this book.

an anonymous channel may be as easy as dropping a letter in a mailbox or walking to a nearby office. In cyberspace, alternative means are available, as we have seen in Section 1.2.2. The trend of wireless connection through handhelds could make it even easier to escape identification. Even if senders over the Internet use methods that enable others to trace their actions without their assistance, it may be very hard, costly, or time-consuming to examine and link the records of Internet access providers and other organizations. The parties that need to be approached to enable tracing may differ in each circumstance, may be in different jurisdictions, may not keep any records at all, and may have no intention of breaching the privacy vows they made to their customers. At the very least, automated key recovery and routine tracing are not an option.

More importantly, and this is the crucial difference with key escrow, users are free to choose for themselves which mechanism and which (and how many) parties they will use for each communication or transaction. With key escrow, in contrast, all system participants are forced to deliver the ability to instantly recover all their secrets to a single set of authorities that they cannot choose freely, and that are under a legal obligation to keep records and cooperate when subpoenaed or presented with a court order or a warrant.

Privacy is protected only if each individual is able at all times to control and determine for him or herself which parties, if any, are capable of recovering a secret. If a user decides to give up some of that control, that is his or her choice, but it should not be hardwired into the design of the system.

The benefits of privacy-enhancing technologies

Oleinick [290, Chapter 4] rightfully notes that "The transfer of control over personal information that occurs in a disclosure of personal information is a transfer of power." Privacy protection requires that each individual has the power to decide how his or her personal data is collected and used, how it is modified, and to what extent it can be linked; only in this way can individuals remain in control over their personal data. The techniques developed in this book demonstrate that these goals can be achieved through the use of privacy-enhancing technologies that are entirely feasible and secure.

When designing abuse protection techniques, it is of fundamental importance that any user secret can be computed only with the consent of that user (unless perhaps if he or she commits a crime). The security techniques described in this book, notably in Section 5.5 and in Section 6.4.4, all meet this objective. In particular, in Section 5.5.1 we have described techniques for *self-revocable* unlinkability and untraceability: certificate holders can prove to have been the originator of a showing protocol execution, can provide evidence to have been the originator of multiple transactions without disclosing their identity, and can prove that they were not involved in certain

transactions.

Organizations often claim that restrictions to the flow of personally identifiable information hinder their ability to use up-to-date personal information for the purpose of reducing identity fraud. Privacy-enhanced PKIs overcome this objection, and in fact offer a myriad of benefits to organizations:

- The need to consult Certificate Revocation Lists or online certificate validation services is minimized.
- CAs and other central parties cannot learn data about the customers of certificate verifiers, and so they cannot compete unfairly. (Organizations typically pay, through discounts or otherwise, to learn the identity and other personal data of customers.)
- The scope for identity fraud and other abuses is minimized.
- Industry-wide adoption of privacy-enhanced PKIs fosters fair competition with respect to the collection and use of personal data. (Organizations can only learn and link data with the consent of the certificate holders to whom the data pertains.)
- The need to protect online databases against intrusions by hackers and insiders is minimized.
- Guaranteed privacy protection makes consumers feel much more comfortable to engage in electronic transactions. Likewise, privacy cultivates goodwill, which is a distinct competitive advantage.
- The trend is for regulations to require mechanisms for assuring adherence of privacy standards. This will significantly raise compliance costs to industry. (See, for example, the Masons Study [256] on compliance with the European Privacy Directive.) The use of privacy-enhanced PKIs enables individuals to reveal only the minimum information needed to complete a transaction, and thus minimizes the burden on industry to demonstrate adherence to privacy standards.
- More generally, privacy-enhanced PKIs are the cheapest and most effective way to comply with as many of the privacy principles of codes of conduct and privacy legislation as possible, since their restrictions and requirements do not apply to anonymous information. In a 1998 report [133], the U.S. Department of Commerce set out the following nine specific characteristics of effective self-regulation for privacy online: awareness, choice, data security, data integrity, consumer access, accountability, verification, consumer recourse, and consequences. Our techniques enable one to implement the first seven of these

in the strongest possible sense. They also facilitate automated dispute resolution (non-repudiation), which greatly helps to realize the privacy characteristics of consumer recourse and consequences.

- The scope for law enforcement intrusions on the data records of organizations is minimized; there will be little to infer.
- Transaction finality is improved.
- The scope for discrimination is greatly reduced.

Adoption of the techniques in this book could also stimulate the public acceptance of smartcards, because smartcards cannot be misused for the purpose of surveillance. Our techniques are desirable even from an economic viewpoint, because they can be implemented using low-cost smartcards without cryptographic coprocessors. Furthermore, tamper-resistant devices for certificate holders are unavoidable if digital signatures are to have a firm legal grounding.

What needs to be done

It is time to stop tolerating (let alone promoting) seal programs, infomediaries, key escrow systems, and other misleading practices towards privacy. Schemes in which users do not have control over their own personal data offer zero privacy. No smoke and mirrors can change this fact.

While privacy-enhancing PKIs minimize the need for legislative intervention, they cannot remove the need for privacy legislation altogether. Privacy legislation is needed to set the general boundaries of what kinds of personal data may be bartered for what purposes,[15] what attribute types may be encoded, under what circumstances (if any) a verifier may refuse access to the holder of a valid certificate, on what grounds (if any) a CA may refuse certificate requests or applicants, and so on. Legislation may also be needed to mandate organizations to delete personal data that has been voluntarily disclosed to them as soon as it has fulfilled the purpose to which the individual consented.[16] Furthermore, legislation is needed to provide a right to judicial remedies, and to enable prosecution of fraudulent behavior (means of redress). Privacy-enhanced PKIs should be the norm, with the kinds of linking and tracing information that may be bartered (and other issues that technology cannot resolve) defined by (preferably overarching) privacy legislation. See the American Civil Liberties Union [10], Clarke [118], and Marx [255, Table II] for discussions of

[15] As we have seen in Section 6.5.5, smartcards can prevent identity bartering, but this is not sufficient.

[16] A precedent for such legislation has been set in 1997 by the Privacy Commissioner of Sweden, who instructed American Airlines operating in Europe to delete all health and medical details on Swedish passengers after each flight unless explicit consent could be obtained; both the District Court and the Court of Appeal have rejected actions by American Airlines.

the kinds of privacy provisions that are desirable. One tantalizing idea that has been put forward is to give individuals property rights over their personal information.

Several influential organizations have in recent years made the case for building privacy into electronic communication and transaction mechanisms. For example:

- In 1995, the NII Task Force [313] stated that "Privacy should not be addressed as a mere afterthought, once personal information has been acquired. Rather, information users should explicitly consider the impact on privacy in the very process of designing information systems and in deciding whether to acquire or use personal information in the first place."

- In 1996, the Working party on Illegal and Harmful Content on the Internet in its report [155] for the Council of Europe stated: "Anonymous use of the Internet takes a number of forms: anonymous browsing, anonymous publishing of content on the World Wide Web, anonymous e-mail messages and anonymous posting of messages to newsgroups. In accordance with the principle of freedom of expression and the right to privacy, use of anonymity is legal. [...] A user should not be required to justify anonymous use."

- Also in 1996, the International Working Group on Data Protection in Telecommunications [217] stated its conviction that "it is necessary to develop technical means to improve the users privacy on the Net. [...] In general users should have the opportunity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service. [...] Anonymity is an essential additional asset for privacy protection on the Internet. Restrictions on the principle of anonymity should be strictly limited to what is necessary in a democratic society without questioning the principle as such."

- In 1997, an advisory committee of the European Commission to the European Parliament [156] recommended that "Technological developments and take-up promotion projects in European Union R&D programmes should concentrate on providing a wide range of interoperable, compatible electronic commerce building-blocks. [...] They should favour technologies which minimise the need for personal data and thus enhance the protection of the right to privacy of consumers (privacy enhancing technologies)."

- Also in 1997, the Working Party of the European Union [373] declared that "where the user can choose to remain anonymous off-line, that choice should also be available on-line. [...] The ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy on-line as they currently enjoy off-line. [...] The principle that the collection of identifiable personal data should be limited to the minimum necessary must be recognized in the evolving national and international laws dealing with the

Internet. It should also be embodied in codes of conduct, guidelines and other 'soft law' instruments that are developed. Where appropriate this principle should specify that individual users be given the choice to remain anonymous."

- In October 1997, Directorate-General XIII of the European Commission [137] warned that privacy safeguards are needed because otherwise "digital signatures could be abused as an efficient instrument for tracing individual on-line consumption patterns and communication or for intercepting, recording or misusing documents or messages."

- In 1998, the Group of Experts on Information Security and Privacy [198], in their background report for an OECD Ministerial Conference, noted: "Privacy enhancing technologies should not be seen as primarily novel technical developments or as additions to existing systems. Rather, they should be seen as a matter of design philosophy: one that encourages (in appropriate circumstances) the removal of identifiers linked to personal data thereby anonymising the data."

- A 1998 draft paper [375] by the U.S. government states: "If electronic commerce is to realize its enormous potential consumers must be confident that their personal information is protected against misuse. Electronic commerce in the next century will thrive only to the extent that individuals' privacy is protected. [...] Technology will offer solutions to many privacy concerns in the online environment, and will serve as an important tool to protect privacy."

- Also in 1998, the Steering Committee of the Federal Public Key Infrastructure [163] warned that "for many applications, identity-based authentication is not only unnecessary, it may be inappropriate. Agencies will need to consider carefully which applications require user authentication (e.g., to protect private information). In many instances, such as downloading forms, anonymous transactions are appropriate."

- In October 1998, the governments of the member countries of the OECD [199] declared that "they will take the necessary steps, within the framework of their respective laws and practices, to ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks, and in particular [...] encourage the use of privacy-enhancing technologies."

Nevertheless, countries have yet to establish a climate that allows privacy-enhancing technologies to flourish. Without efforts to fund and promote the development and adoption of privacy-enhancing technologies, and without the enactment of laws that forbid the use of privacy-invading technologies in communication and transaction applications in which there is no strict need to establish identity, the above statements are nothing more than hollow phrases.

Unfortunately, the benefits of protecting privacy by means of technological measures are not widely acknowledged. Several countries have drafted, or are in the process of drafting, legislation that requires public keys to be bound to true names or traceable pseudonyms. As Baker and Yeo [17] point out, "The effect of these provisions will be to make it more difficult, if not impossible, to establish the legal validity of non-identity certificates and to enforce transactions that are authenticated by non-identity certificates."

The widespread adoption of automated transaction systems that lack any provisions to protect privacy is a very dangerous trend. As Swire [367] points out, "The systems in place in one period can have a powerful effect on what systems will develop in subsequent periods. [...] Once the costs of the database and infrastructure are already incurred for initial purposes, then additional uses may be cost-justified that would not otherwise have been." Holmes [212] notes that "the danger to democratic countries is not that they will openly embrace totalitarianism. It is [...] that they will unwittingly, almost imperceptibly, and with the best of intentions, allow themselves to drift so far in that direction that the final step will then be but a small one." Chaum [104] observes that the current situation "does not want to go halfway in between. It really has a natural tendency to flip into one of two extreme positions." For a compelling case of how only architectures of freedom can prevent tyrannies, see Rummel [331].

Today, the foundations for the communication and transaction technologies of this century are being laid. Digital certificates will be hardwired into all operating systems, network protocols, Web browsers, chipcards, application programs, and so on. To avert the doom scenario of a global village founded wholly on inescapable identification technologies, it is imperative that we rethink our preconceived ideas about security and identity—and build in privacy before the point of no return has been reached.