Foreword

Stefan Brands' Ph.D. thesis, updated and published here in book form, makes major contributions to the state of the art of achieving privacy in an electronic world.

Whit Diffie and Susan Landau, in their excellent book *Privacy on the Line*, proclaim:

> "Privacy encompasses the right to control information about ourselves, including the right to limit access to that information. ... The right to privacy means the right to enjoy solitude, intimacy and anonymity."

Yet today, the identity and on-line behavior of individuals is routinely recorded; users often have little knowledge of or control over such surveillance.

While encryption may protect your credit card number from a wiretapper, it does not prevent the merchant who receives and legitimately decrypts your credit card number from selling it, misusing it, or using it to link the current transaction to a dossier of your previous transactions.

Similarly, conventional public-key digital signatures and certificates can provide reliable identification over a network, so that users can authenticate a merchant's web site and vice versa. An adversary can not impersonate a user, or set up a fraudulent web site, without defeating the digital signature scheme or stealing a secret key. But once you have been reliably identified by your digital signature and corresponding certificate you have lost any hope of remaining anonymous or preventing merchants from cross-linking their records about you.

In cyberspace, the most dangerous threat to your privacy is not a wiretapper, but the other party to your transaction.

While privacy can be enhanced by appropriate legislation and regulation, workable technical approaches, when they can be found, are often more effective. Compare laws against "peeping toms" to window shades!

This book provides new cryptographic communication and transaction techniques so that users can limit the information provided to another party to a bare minimum. For example, a user can remain anonymous while still reliably convincing an information provider that he is a paid subscriber. Moreover, the user's sessions

are "unlinkable"—the information provider cannot even tell if the (anonymous) user currently logged in is the same as the user who logged into some previous session.

Brands' techniques allow an organization or service to issue "credentials" to a user that the user may show anonymously in later sessions. To protect his anonymity maximally, the user may choose to show only a selected portion of any credential he has been issued. To achieve such anonymity, the issuing process is cleverly "blinded" so that the issuer can not identify the user in the later sessions. The issuer may, if he wishes, issue a modified "limited-use" credential that the user can use at most a given number of times. Many extensions and variations are described and discussed.

The cryptographic techniques presented are novel and powerful. They are based on familiar cryptographic foundations such as RSA and the discrete logarithm problem. Brands has invented fascinating new ways of representing certificates and credentials, and proves the security of his techniques using standard cryptographic assumptions.

Brands explains clearly how his new privacy-protecting techniques relate to electronic cash, public-key infrastructures, and smart cards. He also speaks eloquently about the importance of privacy from a larger perspective, and argues against privacy-defeating techniques such as "key escrow."

This book, for both its conceptual framework and technical elaboration, is an important landmark in the evolution of privacy-enhancing technology.

Ronald L. Rivest
Webster Professor of Electrical Engineering and Computer Science
MIT EECS Department
April 30, 2000