NEW SECRET CODES CAN PREVENT A COMPUTERIZED BIG BROTHER

David Chaum

Center for Mathematics and Computer Science (CWI)
Kruislaan 413
1098 SJ Amsterdam, The Netherlands

ABSTRACT

As the use of computers becomes more pervasive, they are capturing increasingly more revealing data about our habits, lifestyles, values, whereabouts, associations, political and religious orientation, etc. The current approach, which requires individuals to identify themselves in relationships with organizations, allows records of all an individual's relationships to be linked and collected together into a dossier or personal profile. Even though such profiles are too extensive to evaluate manually on a mass basis, automated evaluation is becoming increasingly feasible.

A new approach prevents linking of such data, by allowing individuals to conduct relationships under different account numbers or "digital pseudonyms." The pseudonyms are created by a physical random process within a credit-card-sized computer carried by the individual. The card has no secrets from the individual or structure unmodifiable by the individual; it is merely a computer that acts on the individual's behalf and provides a convenient interface.

New cryptographic protocols provide security for both individuals and organizations against abuses by the other. A comprehensive set of three types of consumer transactions can be conducted, each using a different protocol. A communication protocol allows individuals to send and receive confidential and authenticated messages under pseudonyms. But even the tapping of all communication channels and the cooperation of all organizations does not allow messages to be traced to an individual. A payments system protocol allows an individual to pay or be paid, using an account maintained under a pseudonym with a bank. But even cooperation between the bank and other parties to payments does not allow payments to be traced to the individual's account. A credentials protocol allows digitally signed credential statements issued to an

individual under one pseudonym to be transformed into statements that can be shown on the individual's other pseudonyms. But the credentials shown to one organization do not allow tracing of the pseudonyms used with other organizations. All three protocols can be shown by simple mathematical proof to be unconditionally un-traceable, i.e. untraceable no matter how much computation is expended by tracing efforts.

This new approach may actually provide better protection against abuse by individuals, even in areas like consumer credit, social welfare, insurance, etc. than could be acceptably obtained under the current approach. Organizations may favor the new paradigm also because of reduced costs, reduced data maintenance and related exposure, and because of the opportunities for improved good will with advanced computerization. For individuals, the new paradigm offers greater convenience because they can select the card computer that suits them best, the full capabilities of a lost card can conveniently be restored into a replacement card, and the card can protect itself against use by anyone other than its owner. As the public becomes more aware of and familiar with the extent and possibilities of emerging information technology, appreciation of these advantages may grow. Of course an essential advantage of the new approach to individuals is the potential it offers them for regaining monitorability and control over the maintenance and use of information about themselves by others.

REFERENCES

The presentation surveyed the three references. An invitation for journal publication of a survey article has been accepted.

- (1) Chaum, D., "The Dining Cryptographers Problem: Unconditional Sender and Recipient Anonymity," submitted for publication.
- (2) Chaum, D., "Privacy Protected Payments: Unconditional Payer and/or Payee Anonymity," submitted for publication.
- (3) Chaum, D., "Showing Credentials Without Identification: Transferring Signatures Between Unconditionally Unlinkable Pseudonyms," submitted for publication.