

Sidelines

Spy Versus Spy

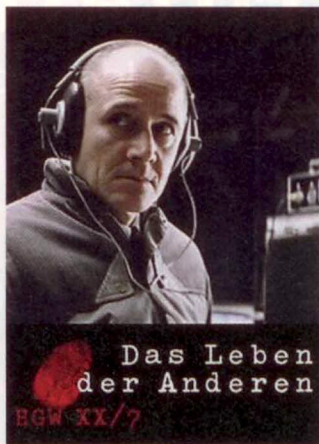
THE CENTURY-OLD ARMS RACE BETWEEN LAW enforcement and privacy is heating up. Who wins? Who should win?

Your answer to the second question depends on who's trying to keep his communications private. In the 2006 movie *Das Leben der Anderen*, the bad guys are the secret police, snooping on dissidents. In the digital battlegrounds of Tehran and Tiananmen, you root for the privacy seekers.

But what if the subject of the bugging is a gang of terrorists planning to blow up a synagogue? Or a crooked governor selling a Senate seat? Then you realize that a victory for privacy would not be an unmixed blessing.

Like it or not, privacy is going to win this battle. One reason is that mathematics favors the cipher. Add a few arithmetic steps to your encrypting program and you slow down your computer by a few seconds but delay the code crackers by a few thousand years. In his column on page 43 Lee Gomes looks at encryption from the everyday perspective of a Microsoft Office user. For people who take the trouble to use long passwords, security has gotten very, very good. On page 40 Andy Greenberg explores a breakthrough in coding that, while purely theoretical today, could someday lead to better privacy in a world where most of your personal computation takes place at a far remove from your desktop.

The other factor is the likely drift of the telephone network to the Internet Protocol, the format used by Skype. Voice over IP converts conversations to packets of bits that can be easily



encrypted with secret keys invented on the fly. Code your phone calls and all the wiretap warrants in the world won't allow the FBI to listen in.

Chief proponent of encrypting phone calls is Philip Zimmermann, whose Zfone software handles all the details. Mainstream phone companies are for now just sniffing at the idea, but it's quite possible that, in a world of IP telephony a decade hence, encryption will become the default option.

Zimmermann is a hero to privacy fans for winning a battle with the government in the 1990s over his Pretty Good Privacy encryption program. The feds thought PGP was so powerful that it should be regulated as a munitions export.

They eventually backed down. They had to. Encryption these days boils down to some well-known computational tricks. It's one thing to stop a missile launcher at the border, quite another to interdict an equation.

Outlaw encryption? That would be not only impossible but a big mistake. So much business these days hangs on secure transmission—your Amazon order, bank wire transfers, government purchasing. Yes, al Qaeda uses encryption. Bank robbers use getaway cars, but that doesn't mean we should outlaw the automobile. In the next century the law enforcers are simply going to have to live without wiretaps.

William Baldwin

Forbes

Editor-in-Chief Steve Forbes

Editors William Baldwin | Paul Maidment

Managing Editors Mia Haugen | Carl Lavin | Stewart Pinkerton | Tom Post | Bruce Upbin

Editor, Forbes Asia Tim W. Ferguson

Executive Editors Dan Bigman | Elizabeth Corcoran | Michael Noer | Larry Reibstein | Tunku Varadarajan | Neil Weinberg | Melanie Wells

Art and Design Director Robert Mansfield • Editorial Counsel Kai Falkenberg • National Editors Quentin Hardy | Janet Novack | Michael K. Ozanian

Department Heads Frederick E. Allen | Mark Decker | Parker Gowan | Steve Kichen | Michael Maiello | Lucy Maher | Deborah Markson-Katz

Robyn Meredith | Matthew Miller | Brett Nelson | Ann Rafalko | Anita Raghavan | Matthew Schifrin

FOUNDED IN 1917

B.C. Forbes, Editor-in-Chief (1917-1954)

Malcolm S. Forbes, Editor-in-Chief (1954-1990)

James W. Michaels, Editor (1961-1999)

July 13, 2009 • Volume 184 • Number 1

FORBES (ISSN 0015 6914) is published biweekly, monthly in July, with an extra issue in September, by Forbes LLC, 60 Fifth Avenue, New York, NY 10011. Periodicals postage paid at New York, NY and at additional mailing offices. Canadian Agreement No. 40036469. Return undeliverable Canadian addresses to DHL Global Mail, 355 Admiral Blvd., Mississauga ON L5T 2N1, Canada. GST # 12576 9513. RT. POSTMASTER: Send address changes to Forbes Subscriber Service, P.O. Box 5471, Harlan, IA 51593-0971.

Subscriptions: U.S.A., one year \$59.95. Canada, one year C\$89.95 (includes GST). Forbes Subscriber Service is always available online. To subscribe, change your address, or for other assistance, please visit www.forbesmagazine.com. You may also write Forbes Subscriber Service, P.O. Box 5471, Harlan, IA 51593-0971 or call 1-515-284-0693. To purchase back issues of Forbes magazine, call 1-212-367-4141.

Mailing List: We make a portion of our mailing list available to reputable firms. If you prefer that we not include your name, please write Forbes Subscriber Service at the address above.

Where necessary, permission is granted by the copyright owner for those registered with the Copyright Clearance Center (CCC), 222 Rosewood Dr., Danvers, MA 01923, to photocopy articles owned by Forbes for a flat fee of \$2.25 per copy per article. Send payment to the CCC stating the ISSN (0015 6914), volume and first and last page number of each article copied. Copying for other than personal use or internal reference, or of articles or columns not owned by Forbes without express permission of Forbes or the copyright owner is expressly prohibited.

To order reprints, call 212-620-2399 or e-mail reprints@forbes.com (minimum order 250). To request permission to republish an article, call 212-620-2434 or fax 212-206-5118. Reprints reproduced by others are not authorized.

Copyright © 2009 Forbes LLC. All rights reserved. Title is protected through a trademark registered with the U.S. Patent & Trademark Office. Printed in U.S.A.