DOI:10.1145/2814825

Peter G. Neumann et al.

Inside Risks

Keys Under Doormats

Mandating insecurity by requiring government access to all data and communications.

Twenty years ago, law enforcement organizations lobbied to require data and communication services to engineer their products to guarantee law enforcement access to all data. After lengthy debate and vigorous predictions of enforcement channels going dark, these attempts to regulate the emerging Internet were abandoned. In the intervening years, innovation on the Internet flourished, and law enforcement agencies found new and more effective means of accessing vastly larger quantities of data. Today, we are again hearing calls for regulation to mandate the provision of exceptional access mechanisms.

In this column, a group of computer scientists and security experts, many of whom participated in a 1997 study of these same topics, explore the likely effects of imposing extraordinary access mandates. We have found the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today's Internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force Internet system developers to reverse forward-secrecy design practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's Internet environment, with millions of apps and globally connected services, means new law enforcement requirements are likely to introduce unanticipated, hard-to-detect security flaws. Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult problems about how such an environment would be governed and how to ensure such systems would respect human rights and the rule of law.

The complexity of today's Internet environment means new law enforcement requirements are likely to introduce unanticipated security flaws.

Political and law enforcement leaders in the U.S. and the U.K. have called for Internet systems to be redesigned to ensure government access to information—even encrypted information. They argue the growing use of encryption will neutralize their investigative capabilities. They propose data storage and communications systems must be designed for exceptional access by law enforcement agencies. These proposals are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm.

As computer scientists with extensive security and systems experience, we believe law enforcement has failed to account for the risks inherent in exceptional access systems. Based on our considerable expertise in real-world applications, we know such risks lurk in the technical details. In this column, we examine whether it is technically and operationally feasible to meet

law enforcement's call for exceptional access without causing large-scale security vulnerabilities. We take no issue here with law enforcement's desire to execute lawful surveillance orders when they meet the requirements of human rights and the rule of law. Our strong recommendation is that anyone proposing regulations should first present concrete technical requirements, which industry, academics, and the public can analyze for technical weaknesses and for hidden costs.

Many of this column's authors worked together in 1997 in response to a similar but narrower and better-defined proposal called the Clipper Chip.[1] The Clipper proposal sought to have all strong encryption systems retain a copy of keys necessary to decrypt information with a trusted third party who would turn over keys to law enforcement upon proper legal authorization. We found at that time it was beyond the technical state of the art to build key escrow systems at scale. Governments kept pressing for key escrow, but Internet firms successfully resisted on the grounds of the enormous expense, the governance issues, and the risk. The Clipper Chip was eventually abandoned. A much narrower set of law-enforcement access requirements has been imposed in the U.S., but only on regulated telecommunications systems. Still, in a small but troubling number of cases, weaknesses related to these requirements have emerged and been exploited by state actors and others. Those problems would have been worse had key escrow been widely deployed. And if all information applications had to be designed and certified for exceptional access, it is doubtful that companies like Facebook and Twitter would even exist. Another important lesson from the 1990s is that the decline in surveillance capacity predicted by law enforcement 20 years ago did not happen. Indeed, in 1992, the FBI's Advanced Telephony Unit warned that within three years Title III wiretaps would be useless: no more than 40% would be intelligible and in the worst case all might be rendered useless.[2] The world did not "go dark." On the contrary, law enforcement has much better and more effective surveillance capabilities now than it did then.

The goal of this column is to similarly analyze the newly proposed requirement of exceptional access to communications in today's more complex, global information infrastructure. We find it would pose far more grave security risks, imperil innovation, and raise difficult issues for human rights and international relations.

There are three general problems. First, providing exceptional access to communications would force a U-turn from the best practices now being deployed to make the Internet more secure. These practices include forward secrecy—where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications. A related technique, authenticated encryption, uses the same temporary key to guarantee confidentiality and to verify the message has not been forged or tampered with.

Second, building in exceptional access would substantially increase system complexity. Security researchers inside and outside government agree that complexity is the enemy of security—every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world. This is a far

IMAGE BY ALICIA KUBISTA/ANDRIJ BORYS ASSOCIATES

more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services, which tend to use similar technologies and are more likely to have the resources to manage vulnerabilities that may arise from new features. Features to permit law enforcement exceptional access across a wide range of Internet and mobile computing applications could be particularly problematic because their typical use would be surreptitious—making security testing difficult and less effective.

Third, exceptional access would create concentrated targets that could attract bad actors. Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. If law enforcement's keys guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege. Moreover, law enforcement's stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple key holders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the U.S. Government Office of Personnel Management (OPM) show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities. In the case of OPM, numerous federal agencies lost sensitive data because OPM had insecure infrastructure. If service providers implement exceptional access requirements incorrectly, the security of all of their users will be at risk.

Our analysis applies not just to systems providing access to encrypted data but also to systems providing access directly to plaintext. For example, law enforcement has called for social networks to allow automated, rapid access to their data. A law enforcement backdoor into a social network is also a vulnerability open to attack and abuse. Indeed, Google's database of surveillance targets was surveilled by Chinese agents who hacked into its systems, presumably for counterintelligence purposes.[3]

The greatest impediment to exceptional access may be jurisdiction. Building in exceptional access would be risky enough even if only one law enforcement agency in the world had it. But this is not only a U.S. issue. The U.K. government promises legislation this fall to compel communications service providers, including U.S.-based corporations, to grant access to U.K. law enforcement agencies, and other countries would certainly follow suit. China has already intimated it may require exceptional access. If a British-based developer deploys a messaging application used by citizens of China, must it provide exceptional access to Chinese law enforcement? Which countries have sufficient respect for the rule of law to participate in an international exceptional access framework? How would such determinations be made? How would timely approvals be given for the millions of new products with communications capabilities? And how would this new surveillance ecosystem be funded and supervised? The U.S. and U.K. governments have fought long and hard to keep the governance of the Internet open, in the face of demands from authoritarian countries that it be brought under state control. Does not the push for exceptional access represent a breathtaking policy reversal?

... legislators should reject out of hand any proposal to return to the failed cryptography control policy of the 1990s.

The need to grapple with these legal and policy concerns could move the Internet overnight from its current open and entrepreneurial model to becoming a highly regulated industry. Tackling these questions requires more than our technical expertise as computer scientists, but they must be answered before anyone can embark on the technical design of an exceptional access system. Absent a concrete technical proposal, and without adequate answers to the questions raised in this column, legislators should reject out of hand any proposal to return to the failed cryptography control policy of the 1990s. C

References

1. Abelson, H. et al. The risks of key recovery, key escrow, and trusted third-party encryption, 1997; http://academiccommons.columbia.edu/catalog/ac:127127.
2. Advanced Telephony Unit, Federal Bureau of Investigation. Telecommunications Overview, slide on Encryption Equipment, 1992; https://www.cs.columbia.edu/~smb/Telecommunications_Overview_1992.pdf.
3. Nakashima, E. "Chinese hackers who breached Google gained access to sensitive data, U.S. officials say." *The Washington Post* (May 20, 2013); http://wapo.st/1MpTz3n.

Harold "Hal" Abelson (hal@MIT.edu) is a professor of electrical engineering and computer science at MIT, a fellow of the IEEE, and a founding director of both Creative Commons and the Free Software Foundation.

Ross Anderson (Ross.Anderson@cl.cam.ac.uk) is Professor of Security Engineering at the University of Cambridge.

Steven M. Bellovin (smb@cs.columbia.edu) is the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University.

Josh Benaloh is Senior Cryptographer at Microsoft Research where his research focuses on verifiable election protocols and related technologies.

Matt Blaze (blaze@cis.upenn.edu) is Associate Professor of Computer and Information Science at the University of Pennsylvania where he directs the Distributed Systems Lab.

Whitfield "Whit" Diffie is an American cryptographer whose 1975 discovery of the concept of public-key cryptography opened up the possibility of secure, Internet-scale communications.

John Gilmore (gnu@eff.org) is an entrepreneur and civil libertarian. He was an early employee of Sun Microsystems, and co-founded Cygnus Solutions, the Electronic Frontier Foundation, the Cypherpunks, and the Internet's alt newsgroups.

Matthew Green (mgreen@cs.jhu.edu) is a research professor at the Johns Hopkins University Information Security Institute. His research focus is on cryptographic techniques for maintaining users' privacy, and on new techniques for deploying secure messaging protocols.

Susan Landau (susan.landau@privacyink.org) is Professor of Cybersecurity Policy at Worcester Polytechnic Institute.

Peter G. Neumann (neumann@csl.sri.com) is Senior Principal Scientist in the Computer Science Lab at SRI International, and moderator of the ACM Risks Forum.

Ronald L. Rivest (rivest@mit.edu) is an MIT Institute Professor, and well known for his co-invention of the RSA public-key cryptosystem, as well for founding RSA Security and Verisign.

Jeffrey I. Schiller (jis@mit.edu) was the Internet Engineering Steering Group Area Director for Security (1994–2003).

Bruce Schneier is a security technologist, author, Fellow at the Berkman Center for Internet and Society at Harvard Law School, and the CTO of Resilient Systems, Inc. He has written a number of books, including *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (Norton, 2015).

Michael A. Specter (specter@mit.edu) is a security researcher and Ph.D. candidate in computer science at MIT's Computer Science and Artificial Intelligence Laboratory.

Daniel J. Weitzner (djweitzner@csail.mit.edu) is Principal Research Scientist at the MIT Computer Science and Artificial Intelligence Lab and Founding Director, MIT Cybersecurity and Internet Policy Research Initiative. From 2011–2012, he was U.S. Deputy Chief Technology Officer in the White House.

The full technical report MIT-CSAIL-TR-2015-026 from which this column has been derived is available at http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

Copyright held by authors.