THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 2 | Number 1 Article 8

2007

Back Matter

BOOK REVIEWS

Gary C. Kessler
Editor
Champlain College
Burlington, VT 05401
gary.kessler@champlain.edu

INTRODUCTION

This issue presents the second Book Review column for the JDFSL. It is an experiment to broaden the services that the journal provides to readers, so we are anxious to get your reaction. Is the column useful and interesting? Should we include more than one review per issue? Should we also review products? Do you have suggested books/products for review and/or do you want to write a review? All of this type of feedback -- and more -- is appreciated. Please feel free to send comments to Gary Kessler (gary.kessler@champlain.edu) or Glenn Dardick (gdardick@dardick.net).

BOOK REVIEW

O'Harrow, R., Jr. (2006). *No Place To Hide*. New York: Free Press. 352 pages, ISBN: 0-7432-8705-3 (paper), US$26

Reviewed by Gary C. Kessler (gary.kessler@champlain.edu)

Personal privacy and the protection of personal identifying information are of concern to all of us. Innumerable articles and conferences address our loss of privacy, either through the sale of consumer databases or our own inattention. Opinions vary from "You have no privacy; get over it" to "This is the end of civil liberties as we know them." We teach people to safely maneuver on the Internet and minimize their exposure to bogus sites set up to steal their identity, warn users about the dangers of phishing and posting personal information on social network sites, use firewalls to protect our databases, and enact laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA) to protect information.

But what are the data custodians doing with the information in their possession? And what about the companies that are mining the vast stores of raw data that are just waiting to be converted to knowledge? Exploring this topic is the *raison d'être* of this book, written by a financial reporter for the *Washington Post*. This book -- and the accompanying Web site at *http://www.noplacetohide.net/* -- is an essential read for anyone interested in knowing about commercial organizations and governmental agencies that collect information about all of us, and what they are do with this information, regardless of your opinion about this activity.

The book's introduction starts at the International Association of Chiefs of Police (IACP) technology conference in August, 2003 and the array of technologies for snooping and/or intelligence gathering on display there. That was just foreshadowing the rest of the book, of course, because the story really begins on September 11, 2001 and perspectives seen through the eyes of individuals that include an Assistant U.S. Attorney General, a U.S. Senator, and a staffer at a public advocacy group. The debate about the trade-off between privacy in a free society and the legitimate needs of the government to combat crime and defend the country against enemies, both foreign and domestic, has been ongoing since the early days of our nation. The aftermath of 9/11, however, presented a unique opportunity where it seemed that most of the people in the U.S. were willing to exchange civil rights for additional "security" -- a climate where the U.S.A. PATRIOT Act could be written and enacted in a matter of weeks. The first chapter, aptly titled "Six Weeks in Autumn," sets the stage for the rest of the book and reminds the reader about the discussion in the days immediately following 9/11 and the legislative and executive response to the new era in which we found ourselves.

The rest of the book tells a story of data collection and sharing, using technologies that were developed largely in the 1990s but were hard to sell to a population primarily concerned with civil liberties. Priorities changed after September 11.

One company we read about is Acxiom, a major player in the data collection business. Storing more than a petabyte (10^{15} bytes) of information about roughly 200 million adults in the U.S. gathered from its client records, Acxiom helps its clients target customers, screen potential employees, find deadbeats, and, ostensibly, predict a consumer's behavior. Although commercial in nature, this technology and data was offered to the government in the days following 9/11, tremendously augmenting what the government knew about its citizens.

We also read about Data Base Technologies (DBT), a company started in the 1990s to track Florida automobile records. Next they got the contract to maintain driver's licenses. Corporate records followed, then property transactions, and professional licenses, and more and more until they grew to have more than eight billion files on people around the country. ChoicePoint, a spin-off of credit bureau giant, Equifax, purchased DBT and expanded their own operation, eventually playing a role maintaining criminal and voting records -- and errors that caused many voters in Florida to be improperly disenfranchised during the 2000 Presidential election. We read about the difficulty in ensuring that the records in these databases are accurate and the harder task of correcting any errors that have rippled through many databases.

From DBT also came Seisint, a direct marketing company that used many advanced data mining techniques to target customers. Post-9/11, Seisint created a service for law enforcement and the anti-terrorism community called the

Multi-state Anti-Terrorism Information Exchange -- dubbed *Matrix* -- which can bring up an incredible amount of information on just about anyone, ranging from financial and medical records to criminal records and photographs.

Conceptually, all of these broad scope databases match a plan first floated in the late 1990s called Total Information Awareness (TIA). The TIA vision was to give the intelligence community the ability to acquire as much information about everything as possible -- travel records, financial transactions, phone calls, e-mail and text messages, technology and chemical purchases, and more -- so that analysts could detect nefarious patterns of behavior; consider what might have happened if the government had known prior to 9/11 that a group of men were attending flight school with particular interest in flying large planes but seemingly uninterested in taking off and landing. A curiosity when first proposed, TIA resurfaced after 9/11 and its vision is very much alive today.

Other chapters deal with equally important issues, such as the use of biometrics (such as facial recognition) to complement an ever-increasing array of cameras used to provide monitoring and surveillance in high-risk or high-security areas. We also read about databases currently in use by the Transportation Security Administration (TSA) such as CAPPS II and the Non-Obvious Relationship Awareness (NORA) program, and we once again hear about giant commercial database companies such as Acxiom, ChoicePoint, and LexisNexis.

Chapter Ten, "No Place To Hide," wraps the book up by noting the many ways in which our privacy is compromised in subtle, yet pervasive, ways -- credit cards, ATM cards, magnetic strips on store discount and public transportation cards, RFID chips for gas purchases and toll booths, GPS-enabled cell phones and automobiles in constant contact with the network, surveillance cameras everywhere... and the list goes on and on.

This book is very well-written, well-documented, and reads like a novel. The discussion of individuals, as well as companies, puts this story on a very personal level. The information laid out here certainly shows why organizations such as the American Civil Liberties Union (ACLU) and Electronic Privacy Information Center (EPIC) think that they have their work cut out for themselves. And, it could be argued, this book is written to support the civil libertarian view.

Nevertheless, the book is an essential read for informed debate. It is clear that we have all sacrificed enormous amounts of privacy as we have entered the electronic information age. Some of our privacy has been surrendered for our own *convenience* but much has been lost without our knowledge. Do we trust the custodians? Are we safer or more secure? The debate might rage on, but the more information we have, the better.

Subscription Information

The Journal of Digital Forensics, Security and Law (JDFSL) is a publication of the Association of Digital Forensics, Security and Law (ADFSL). The Journal is published on a non-profit basis. In the spirit of the JDFSL mission, individual subscriptions are discounted. However, we do encourage you to recommend the journal to your library for wider dissemination.

The journal is published in both print and electronic form under the following ISSN's:

ISSN: 1558-7215 (print)

ISSN: 1558-7223 (online)

Subscription rates for the journal are as follows:

Institutional - Print & Online: $395 (4 issues)

Institutional - Online only: $295 (4 issues)

Individual - Print & Online: $80 (4 issues)

Individual - Online only: $25 (4 issues)

Subscription requests may be made to the ADFSL.

The offices of the Association of Digital Forensics, Security and Law (ADFSL) are at the following address:

Association of Digital Forensics, Security and Law
Longwood University
201 High Street
Farmville, Virginia 23909
Tel: 434-395-2377
Fax: 434-395-2203
E-mail: editor@jdfsl.org
Website: http://www.adfsl.org

Announcements and Upcoming Events

2007 Conference on Digital Forensics, Security and Law

Arlington, Virginia USA
April 18-20, 2007

The ADFSL 2007 Conference on Digital Forensics, Security and Law will be held in Arlington, Virginia USA on April 18-20, 2007.

http://www.digitalforensics-conference.org

ECEG 2007 – 7th European Conference on e-Government

Haagse Hogeschool, Den Haag, The Netherlands
21-22 June 2007

ECEG 2007 includes a mini track on legal, agency, trust and governance issues in e-Government. Submissions are invited from academics, government departments and practitioners in the public and private sector. the call for papers and registration details can be found on the conference website.

A 10% discount on attendance is available to JDFSL readers (minimum charge of $350). Enter IWJDFSL10 in the discount code box on the online registration form.

http://www.academic-conferences.org/eceg/eceg2007/eceg2007-minitrack.htm

ECIW 2007 – 6th European Conference on Information Warfare and Security

Defence College of Management and Technology, Shrivenham, UK
July 2-3, 2007

Mini-Track on Forensic Computing
Track chair: Dr Jill Slay, Enterprise Security Management Lab, university of South Australia

http://www.academic-conferences.org/eciw/eciw2007/eciw07-abstract-submission.htm

5th Australian Digital Forensics Conference 2007 (ADFC2007)

ADFC2007 will be held Monday, December 3rd, 2007 at Edith Cowan University, Mount Lawley, Western Australia. The aim of ADFC 2007 is to bring together IT managers, system and network administrators, security specialists, academics, security solutions vendors, practitioners and anyone interested in:

- Computer forensics its role and application
- Techniques in detecting, responding and investigating computer and related security incidents
- Sharing their views, experiences and knowledge with those involved in the computer forensic field

All papers must be submitted via the conference website. For more detailed information regarding submissions requirements, please visit the website at
http://scissec.scis.ecu.edu.au/conferences2007

The 5th Australian Digital Forensics Conference will be run in conjunction with 8th Australian Information Warfare and Security, and the 5th Australian Information Security Management Conference jointly from 3rd - 4th December, 2007 at ECU Western Australia.

Journal of Digital Forensics, Security and Law

Volume 2, Number 1

2007

Contents