Protecting Privacy in Video Surveillance

Andrew Senior
Editor

Protecting Privacy in Video Surveillance

Springer

Editor
Andrew Senior
Google Research, New York
USA
a.senior@ieee.org

ISBN 978-1-84882-300-6 e-ISBN 978-1-84882-301-3
DOI 10.1007/978-1-84882-301-3
Springer Dordrecht Heidelberg London New York

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2009922088

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

Fueled by growing asymmetric/terrorist threats, deployments of surveillance systems have been exploding in the 21st century. Research has also continued to increase the power of surveillance, so that today's computers can watch hundreds of video feeds and automatically detect a growing range of activities. Proponents see expanding surveillance as a necessary element of improving security, with the associated loss in privacy being a natural if unpleasant choice faced by society trying to improve security. To the surprise of many, a 2007 federal court ruled that the New York Police must stop the routine videotaping of people at public gatherings unless there is an indication that unlawful activity may occur. Is the continuing shift to a surveillance society a technological inevitability, or will the public backlash further limit video surveillance?

Big Brother, the ever-present but never seen dictator in George Orwell's *Nineteen Eighty-Four*, has been rated as one of the top 100 villains of all time and one of the top 5 most influential people that never lived. For many the phrase "Big Brother" has become a catch-phrase for the potential for abuse in a surveillance society. On the other hand, a "Big Brother" can also be someone that looks out for others, either a literal family member or maybe a mentor in a volunteer program.

The diametric interpretations of "Big Brother", are homologous with the larger issue in surveillance. Video surveillance can be protective and beneficial to society or, if misused, it can be intrusive and used to stifle liberty. While policies can help balance security and privacy, a fundamental research direction that needs to be explored, with significant progress presented within this book, challenges the assumption that there is an inherent trade-off between security and privacy.

The chapters in this book make important contributions in how to develop technological solutions that simultaneously improve privacy while still supporting, or even improving, the security systems seeking to use the video surveillance data. The researchers present multiple win-win solutions. To the researchers whose work is presented herein, thank you and keep up the good work. This is important work that will benefit society for decades to come.

There are at least three major groups that should read this book. If you are a researcher working in video surveillance, detection or tracking, or a researcher in social issues in privacy, this is a must-read. The techniques and ideas presented could transform your future research helping you see how to solve both security

and privacy problems. The final group that needs to read this book are technological advisors to policy makers, where it's important to recognize that there are effective alternatives to invasive video surveillance. When there was a forced choice between security and privacy, the greater good may have lead to an erosion of privacy. However, with the technology described herein, that erosion is no longer justified. Policies need to change to keep up with technological advances.

It's a honor to write a Foreword for this book. This is an important topic, and is a collection of the best work drawn from an international cast of preeminent researchers. As a co-organizer of the first IEEE Workshop on Privacy Research in Vision, with many of the chapter authors presenting at that workshop, it is great to see the work continue and grow. I hope this is just the first of many books on this topic – and maybe the next one will include a chapter by you.

El Pomar Professor of Innovation and Security,
University of Colorado at Colorado Springs Chair,
IEEE Technical Committee on Pattern
Analysis and Machine Intelligence

Terrance Boult
April 2009

Preface

Privacy protection is an increasing concern in modern life, as more and more information on individuals is stored electronically, and as it becomes easier to access and distribute that information. One area where data collection has grown tremendously in recent years is video surveillance. In the wake of London bombings in the 1990s and the terrorist attacks of September 11th 2001, there has been a rush to deploy video surveillance. At the same time prices of hardware have fallen, and the capabilities of systems have grown dramatically as they have changed from simple analogue installations to sophisticated, "intelligent" automatic surveillance systems.

The ubiquity of surveillance cameras linked with the power to automatically analyse the video has driven fears about the loss of privacy. The increase in video surveillance with the potential to aggregate information over thousands of cameras and many other networked information sources, such as health, financial, social security and police databases, as envisioned in the "Total Information Awareness" programme, coupled with an erosion of civil liberties, raises the spectre of much greater threats to privacy that many have compared to those imagined by Orwell in "1984".

In recent years, people have started to look for ways that technology can be used to protect privacy in the face of this increasing video surveillance. Researchers have begun to explore how a collection of technologies from computer vision to cryptography can limit the distribution and access to privacy intrusive video; others have begun to explore mechanisms protocols for the assertion of privacy rights; while others are investigating the effectiveness and acceptability of the proposed technologies.

Audience

This book brings together some of the most important current work in video surveillance privacy protection, showing the state-of-the-art today and the breadth of the field. The book is targeted primarily at researchers, graduate students and developers in the field of automatic video surveillance, particularly those interested in the areas of computer vision and cryptography. It will also be of interest to

those with a broader interest in privacy and video surveillance, from fields such as social effects, law and public policy. This book is intended to serve as a valuable resource for video surveillance companies, data protection offices and privacy organisations.

Organisation

The first chapter gives an overview of automatic video surveillance systems as a grounding for those unfamiliar with the field. Subsequent chapters present research from teams around the world, both in academia and industry. Each chapter has a bibliography which collectively references all the important work in this field.

Cheung et al. describe a system for the analysis and secure management of privacy containing streams. Senior explores the design and performance analysis of systems that modify video to hide private data. Avidan et al. explore the use of cryptographic protocols to limit access to private data while still being able to run complex analytical algorithms. Schiff et al. describe a system in which the desire for privacy is asserted by the wearing of a visual marker, and Brassil describes a mechanism by which a wireless Privacy-Enabling Device allows an individual to control access to surveillance video in which they appear. Chen et al. show conditions under which face obscuration is not sufficient to guarantee privacy, and Gross et al. show a system to provably mask facial identity with minimal impact on the usability of the surveillance video. Babaguchi et al. investigate the level of privacy protection a system provides, and its dependency on the relationship between the watcher and the watched. Hayes et al. present studies on the deployment of video systems with privacy controls. Truong et al. present the BlindSpot system that can prevent the capture of images, asserting privacy not just against surveillance systems, but also against uncontrolled hand-held cameras.

Video surveillance is rapidly expanding and the development of privacy protection mechanisms is in its infancy. These authors are beginning to explore the technical and social issues around these advanced technologies and to see how they can be brought into real-world surveillance systems.

Acknowledgments

I gratefully acknowledge the support of my colleagues in the IBM T.J.Watson Research Center's Exploratory Computer Vision group during our work together on the IBM Smart Surveillance System and the development of privacy protection ideas together: Sharath Pankanti, Lisa Brown, Arun Hampapur, Ying-Li Tian, Ruud Bolle, Jonathan Connell, Rogerio Feris, Chiao-Fe Shu. I would like to thank the staff at Springer for their encouragement, and finally my wife Christy for her support throughout this project.

The WITNESS project

Royalties from this book will be donated to the WITNESS project (witness.org) which uses video and online technologies to open the eyes of the world to human rights violations.

New York *Andrew Senior*

Contents

Contributors

Shai Avidan Adobe Systems Inc., Newton, MA, USA, avidan@adobe.com

Noboru Babaguchi Deparment of Communication Engineering, Osaka University, Suita, Osaka 565-0871, Japan, babaguchi@comm.eng.osaka-u.ac.jp

Simon Baker Microsoft Research, Microsoft Corporation, Redmond, WA 98052, USA, sbaker@microsoft.com

Jack Brassil HP Laboratories, Princeton, NJ 08540, USA, jtb@hpl.hp.com

Yi Chang School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA, changyi@cs.cmu.edu

Datong Chen School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA, datong@cs.cmu.edu

S.-C.S. Cheung Center for Visualization and Virtual Environments, University of Kentucky, Lexington, KY 40507, USA, cheung@engr.uky.edu

Jeffrey Cohn Department of Psychology, University of Pittsburgh, Pittsburgh, PA, USA, jeffcohn@pitt.edu

Ariel Elbaz Columbia University, New York, NY, USA, arielbaz@cs.columbia.edu

Ken Goldberg Faculty of Departments of EECS and IEOR, University of California, Berkeley, CA, USA, goldberg@berkeley.edu

Ralph Gross Data Privacy Lab, School of Computer Science,Carnegie Mellon University, Pittsburgh, PA, USA, rgross@cs.cmu.edu

Gillian R. Hayes Department of Informatics, Donald Bren School of Information and Computer Science, University of California, Irvine, CA 92697-3440, USA, gillianrh@ics.uci.edu

Takashi Koshimizu Graduate School of Engineering, Osaka University, Suita, Osaka 565-0871, Japan

Tal Malkin Columbia University, New York, NY, USA, tal@cs.columbia.edu

Marci Meingast Department of EECS, University of California, Berkeley, CA, USA, marci@eecs.berkeley.edu

Ryan Moriarty University of California, LA, USA, ryan@cs.ucla.edu

Deirdre K. Mulligan Faculty of the School of Information, University of California, Berkeley, CA, USA, dmulligan@law.berkeley.edu

T. Nguyen School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR 97331, USA

J.K. Paruchuri Center for Visualization and Virtual Environments, University of Kentucky, Lexington, KY 40507, USA

Shwetak N. Patel Computer Science and Engineering and Electrical Engineering, University of Washington Seattle, WA 98195, USA, shwetak@cs.washington.edu

Shankar Sastry Faculty of the Department of EECS, University of California, Berkeley, CA, USA, sastry@eecs.berkeley.edu

Jeremy Schiff Department of EECS, University of California, Berkeley, CA, USA, jschiff@eecs.berkeley.edu

Andrew Senior Google Research, New York, USA, a.senior@ieee.org

Jay W. Summet College of Computing & GVU, Center Georgia Institute of Technology Atlanta, GA 30332, USA summetj@cc.gatech.edu

Latanya Sweeney Data Privacy Lab, School of Computer Science,Carnegie Mellon University, Pittsburgh, PA, USA, latanyag@cs.cmu.edu

Tomoji Toriyama Advanced Telecommunications Research Institute International, Kyoto, Japan

Fernando de la Torre Robotics Institute, Carnegie Mellon University, Pittsburgh, PA, USA, ftorre@cs.cmu.edu

Khai N. Truong Department of Computer Science, University of Toronto, Toronto, ON M5S 2W8, Canada, khai@cs.toronto.edu

Ichiro Umata National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan

M.V. Venkatesh Center for Visualization and Virtual Environments, University of Kentucky, Lexington, KY 40507, USA

Rong Yan School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA, yanrong@cs.cmu.edu

Jie Yang School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA, yang@cs.cmu.edu

J. Zhao Center for Visualization and Virtual Environments, University of Kentucky, Lexington, KY 40507, USA