Cybersurveillance in a Post-Snowden World

Carolina Academic Press
Global Papers Series

Edited by
Russell L. Weaver and Steven I. Friedland

Volume I
Recent Developments in Administrative Law and Alternative Dispute Resolution

Volume II
Comparative Perspectives on Freedom of Expression

Volume III
Comparative Perspectives on Administrative Procedure

Volume IV
Privacy in a Digital Age

Volume V
Comparative Perspectives on Remedies

Volume VI
Cybersurveillance in a Post-Snowden World

Cybersurveillance in a Post-Snowden World

Balancing the Fight Against Terrorism Against Fundamental Rights

---

Global Papers Series
Volume VI

Edited by

Russell L. Weaver
Professor of Law & Distinguished University Scholar
University of Louisville
Louis D. Brandeis School of Law

Steven I. Friedland
Professor of Law & Senior Scholar
Elon University School of Law

Arnaud Raynouard
Professor of Law
Université Paris Dauphine

Duncan Fairgrieve
Professor of Law, British Institute of International &
Comparative Law & Associate Professor of Law
Université Paris Dauphine

Carolina Academic Press
Durham, North Carolina

Print ISBN: 978-1-5310-0597-9
Ebook ISBN: 978-1-5310-0598-6

Library of Congress Cataloging-in-Publication Data

Names: Weaver, Russell L., 1952-, editor.
Title: Cybersurveillance in a post-Snowden world : balancing the fight against terrorism against fundamental rights / Edited by Russell L. Weaver, Steven I. Friedland, Arnaud Raynouard, and Duncan Fairgrieve.
Description: Durham, North Carolina : Carolina Academic Press, 2017. | Series: The global papers series ; volume vi
Identifiers: LCCN 2017014441 | ISBN 9781531005979 (alk. paper)
Subjects: LCSH: Electronic surveillance--Law and legislation. | Civil rights. | Terrorism--Prevention.
Classification: LCC K5480 .C93 2017 | DDC 345/.052--dc23
LC record available at https://lccn.loc.gov/2017014441

Carolina Academic Press, LLC
700 Kent Street
Durham, North Carolina 27701
Telephone (919) 489-7486
Fax (919) 493-5668
www.cap-press.com

Printed in the United States of America

Contents

Series Note

The Global Papers Series involves publications of papers by nationally and internationally prominent legal scholars on a variety of important legal topics, including administrative law, freedom of expression, defamation and criminal law. The books in this series present the work of scholars from different nations who bring diverse perspectives to the issues under discussion.

Russell L. Weaver,[1]
Duncan Fairgrieve,[2]
Steven I. Friedland[3]

Introduction: Cybersurveillance Discussion Forum– Balancing the Fight Against Terrorism Against Fundamental Rights

This book consists of "discussion papers" submitted and discussed at the Cybersurveillance Discussion Forum that was held in Paris, France, on June 15–16, 2016, at the Université Paris Dauphine. The event was sponsored by the Université Paris—Dauphine, the Washington & Lee University School of Law, the Emory University School of Law, The University of Alabama School of Law, the Elon University School of Law, and the University of Louisville's Louis D. Brandeis School of Law. The papers covered an array of topics. Nevertheless, a constant theme throughout the papers was the effort to find a balance between the need to combat terrorism, and the societal and individual interests in privacy and freedom from government surveillance. The papers published here examine these issues from French, Spanish, American, Hungarian and British perspectives. The project was hampered by the fact that governments frequently conduct surveillance operations in secrecy so that citizens have little impact or oversight, or even adequate knowledge regarding what their governments are doing.

Ms. Mariette Jones, Senior Lecturer in Law at Middlesex University, submitted an article entitled *Double-Lock or Double-Bind? The Investigatory Powers Bill and Freedom of Expression in the United Kingdom*. In her article, she ex-

---

1. Professor of Law & Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law.

2. Professor of Law, British Institute of International & Comparative Law & Associate Professor of Law, Université Paris Dauphine.

3. Professor of Law & Senior Scholar, Elon University School of Law.

plores the cybersurveillance situation in the UK, noting that Snowden's revelations regarding the US National Security Agency's (NSA) widespread cybersurveillance operation reverberated through the UK, in much the same way that they reverberated through the rest of the world, and presented the British with a similar dilemma regarding the balance between privacy and security. In the article, she examines the Investigatory Powers Bill (IP Bill) that was being considered by Parliament. The IP Bill provides for the interception and monitoring of communications data, as well as for a "double lock" provision which is designed as a "safeguard against abuses and a guarantor of due process," and the bill's provisions for secrecy. The article puts aside the very real privacy concerns raised by the IP Bill, which are being thoroughly examined elsewhere, and focuses instead on the bill's implications for freedom of expression. In the process, she discusses the extensive cybersurveillance operation already in place in the UK. She concludes by noting that the UK has been willing to trade off civil rights in an effort to prevent terrorism, but she wonders whether the absence of major terrorist acts in the UK reveals the effectiveness of the UK's covert and overt surveillance actions.

Professor Duncan Fairgrieve of the British Institute of International and Comparative Law, and Université Paris Dauphine, submitted a joint article (with professors Weaver, Koltay and Friedland) entitled *Cybersurveillance: American, Hungarian and British Perspectives*. In his contribution to this article, Professor Fairgrieve also examines the cybersurveillance situation in the UK. He agrees with Ms. Jones that, like many other nations, Britons were surprised by Edward Snowden's revelations regarding the scope of the NSA's governmental cybersurveillance, as well as by the scope of the UK's own cybersurveillance operation. He notes that the legal response in the UK is complicated by the lack of one single constitutional document, and that common law constraints on executive action have foundered because of the complexity of the pre-existing framework which failed to establish a right to protection for private communications. He then notes that ECtHR case law has held that the collection of communications data and the interception of the contents of communications interferes with Article 8, but the ECtHR has not held that "bulk data collection and analysis, in the absence of suspicion, is not in itself a disproportionate interference with the right to respect for private life." He then examines the statutory authority in the UK for the interception of telecommunications or communications data is provided by the Regulation of Investigatory Powers Act 2000 ("RIPA"). Although it is in principle illegal to intercept communications, or to obtain information about the use made of a telecommunications service without the consent of the user, RIPA provides

certain public authorities with the statutory authority to collect and analyze communications. He then discusses the mechanisms by which warrants are issued, and the types of warrants that can be issued.

Professor Fairgrieve notes that the UK has attempted to build various safeguards and oversight procedures into its cybersurveillance mechanisms. For example, the Interception of Communications Commissioner is responsible for reviewing the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities. The IOCC thus holds the public authorities that exercise RIPA powers to account and seeks to improve compliance by means of scrutiny. The Commissioner is a serving or retired judge who reports to the Prime Minister on a half-yearly basis with respect to the carrying out of the Interception of Communications Commissioner's functions. Professor Fairgrieve also discusses the Investigatory Powers Tribunal which was established under RIPA to investigate and determine complaints of unlawful use of interception of communications and gathering of communications data, as well as complaints under Section 7 of the HRA in respect of intelligence or law enforcement agencies. He also focuses on the Five Eyes Partnership (that includes the UK, Australia, Canada, New Zealand, and the USA) which requires judicial authorization for cybersurveillance. Finally, he examines the proposed legislation which imposes a "double lock" system which means that warrants must be issued by the Secretary of State but do not come into force until approved by a Judicial Commissioner (composed of former or serving judges), who review the proposed order. However, as he notes, it is not clear that the "double-lock" provides a suitable safeguard on the exercise of power because the balance of power to authorize weighs too heavily in favor of the executive. Judicial Commissioners are executive-driven and therefore do not have judicial independence.

Professor Russell Weaver of the University of Louisville and Professor Steve Friedland of the Elon University School of Law joined Professor Fairgrieve on the article entitled *Cybersurveillance: American, Hungarian and British Perspectives*. They note that the situation in the U.S. is ironic because, although the United States Constitution was founded based upon a distrust of government, the U.S. National Security Agency (NSA) has been engaged in a massive cybersurveillance operation that was being conducted almost entirely in secret. The article notes that the Fourth Amendment to the United States Constitution, which provides a seeming limitation on the scope of cybersurveillance authority, has proven to be relatively ineffectual in terms of limiting governmental authority. They also note the extent of privacy surveillance.

Professor Andras Koltay, of Pázmány Péter Catholic University Faculty of Law (Hungary), also joined the article entitled *Cybersurveillance: American, Hungarian and British Perspectives*. In his contribution, Professor Koltay examines the Hungarian situation. Hungary is unique in that state protections against governmental intelligence operations were developed only after the collapse of the Communist regime in 1990. However, as with other nations, Hungary began to engage in greater surveillance following the latest emergence of terrorism on the continent. After 2010, Hungary altered its law on the collection of intelligence information. He notes that Article VI (1) of the Fundamental Law provides comprehensive protections for privacy, including the private and family life of individuals, their homes, their social contacts and reputations, and that there is a close relationship between the right to privacy afforded by Article VI (1) of the Fundamental Law and the right to human dignity guaranteed by Article II of the Fundamental Law. He goes on to note that Hungary's Constitutional Court has outlined general criteria governing the means and methods of collecting intelligence information that are acceptable under the democratic rule of law. The broad-ranging rules governing intelligence instruments are set forth in the individual acts governing the bodies authorized to use them, including the Police Act, the Act on the National Security Services, the Act on the Criminal Procedure, the Act on the Public Prosecutor's Office and the Act on the National Tax and Customs Authority.

The Hungarian regulation in effect provides for two different processes for collecting intelligence information: one for *law enforcement purposes* and the other for *purposes other than law enforcement*. Collection of intelligence information for purposes other than law enforcement may be subject to external authorization or it might not be. When authorization is required by law, the authorization must come from a judge or the Minister of Justice. When the government seeks to detect a specific crime, the collection of intelligence information must be authorized by a judge appointed by the Chairman of the Metropolitan Court of Budapest. Other activities, involving the general collection of information, must be authorized by the Minister of Justice. Collection of intelligence information is allowed if the data is required to perform tasks mandated by law that cannot be acquired in other ways. However, it is possible to obtain exceptional authorization under Article 59 of Act on the National Security Services. If the delay caused by the authorization procedure would deprive the Security Services of the chance to detect crime, or uncover evidence in a specific case, the interests of the effective operation of the National Security Service, the General Director of the National Security Service can authorize the collection of in-

telligence information under Article 56, parallel with the submission of a proposal for the authorization, pending the decision of the Minister of Justice or the judge.

The Hungarian surveillance system was challenged in Constitutional Court Decision No. 323/2013. (VI. 22.), in which the applicants challenged the collection of intelligence information by the counter terrorism body for purposes other than law enforcement, claiming that the challenged provision violated the Fundamental Law because it allows the counter-terrorism bodies to collect intelligence information without ensuring the enforcement of fundamental rights. The Constitutional Court held that the right to the protection of privacy and the right of informational self-determination are not unrestricted fundamental rights. Intrusion on privacy and the use of data can be justified by both law enforcement and national security objectives. In the meanwhile, the individual is required to tolerate the restriction of fundamental rights to the extent the restriction has a legal constitutional basis. In the opinion of the Constitutional Court, national security tasks include a much wider range of activities than just law enforcement tasks, and the country has a legitimate interest in detecting and preventing individuals from committing certain acts even if the individuals may not have committed specific crimes. However, the Parliament's National Security Committee exercises control over the counter-terrorism body's activities, performed through application of the rules set forth in the Act on National Security Services.

Professor Cristina Pauner Chulvi, of the University Jaume I in Castellón (Spain), focuses on the increasing use of drone technology (also known as unmanned aerial vehicles (UAV) or remotely piloted aircraft systems (RPAS)) in society. She argues that, while drones "constitute a promising technology with potential benefits for European industries and citizens," "they are also of concern because of their potential impact on privacy and data protection." In her article, she notes that drones are increasingly being used by both civilians and government as a way to gather information. While she concludes that the benefits of drones are undeniable, she notes that drones have enormous privacy implications because they can employ extremely sophisticated technologies, including "high-power zoom lenses, night vision, infrared, ultraviolet, thermal imaging, and radar technologies, video analytic technology, speakers capable of monitoring personal conversations, distributed video or facial and other soft biometric recognition." These capabilities allow the government "to take aerial photographs with high definition, for monitoring crowds at events such as protests or sporting, hacking WI-FI networks to intercept communications, the identification of

criminals or the monitoring of the suspects." She concludes that "the security concept is being interpreted in such a broad sense that it allows national legislation to evade provisions on privacy and data protection," and that there is a need for appropriate limitations on the use of drones for collecting information.

Professor Rosario Serra-Cristóbal, of the University of Valencia, submitted an article entitled *Surveillance on Data and Electronic Communications in the Counter-Terrorism Fight in Spain.* In that article, she seeks to "highlight the necessity to respect both commonly accepted principles governing data processing and the rule of law when monitoring communications and people's data in counter-terrorism," focusing on the 2015 amendments to Spain's cybersurveillance law. She begins by noting that a certain level of surveillance is necessary in the fight against terrorism, and discusses Spain's National Security Act enacted in 2015. However, she goes on to argue that "it is imperative to determine which risks and threats to security, justify restrictions on human rights and under what conditions" because of "the risk of overreacting to terrorism." She concludes that, if we ignore our fundamental rules, then we will lose the war against terrorism.

The paper by Professor Anne Debet of the University of Paris Descartes, entitled *Cybersurveillance by Law Enforcement Authorities After the Digital Rights Judgment: The Impact on French Law*, examines the situation in France. As in other nations, France has limited the right of privacy in an effort to fight terrorism. In the *Digital Rights* case, the European Court invalidated the Digital Rights Directive on human rights grounds, focusing on the right to privacy. In her view, French authorities have been "deaf" in terms of their willingness to take account of the major role being played by the ECJ on human rights matters. She expresses hope that "in the future, the council will also realize the place that should be given to ECJ case law!"

The final article, Professor Olivia Tambou's *Profiling in the General Data Protection Regulation: Progress, But More Improvements Are Needed,* discusses the scope of the European Union's Data Protection Regulation. The article examines the fact that both public authorities and private entities routinely track personal data in order to analyze individual behavior. She then discusses how this tracking has led to profiling and big data analysis. She then analyzes how these activities are analyzed under European law.