



The War on Privacy

The War on Privacy

Jacqueline Klosek

PRAEGER

Westport, Connecticut
London

Library of Congress Cataloging-in-Publication Data

Klosek, Jacqueline, 1972-

The war on privacy / Jacqueline Klosek.

p. cm.

Includes bibliographical references and index.

ISBN 0-275-98891-0 (alk. paper)

1. Privacy, Right of. 2. War on Terrorism, 2001—Law and legislation. 3. Privacy, Right of—United States. 4. War on Terrorism, 2001—Law and legislation—United States. I. Title.

K3263.K56 2007

342.08'58—dc22

2006028565

British Library Cataloguing in Publication Data is available.

Copyright © 2007 by Jacqueline Klosek

All rights reserved. No portion of this book may be reproduced, by any process or technique, without the express written consent of the publisher.

Library of Congress Catalog Card Number: 2006028565

ISBN 10: 0-275-98891-0

ISBN 13: 978-0-275-98891-3

First published in 2007

Praeger Publishers, 88 Post Road West, Westport, CT 06881

An imprint of Greenwood Publishing Group, Inc.

www.praeger.com

Printed in the United States of America



The paper used in this book complies with the Permanent Paper Standard issued by the National Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

To Grace Young, a true friend and inspiration.
Your support, friendship and laughter has meant everything.

Any society that would give up a little liberty to gain a little security
will deserve neither and lose both.

—*Benjamin Franklin*

Contents

	<i>Preface</i>	xi
	Introduction	i
One	Privacy in the United States Prior to September 11	13
Two	War on Terrorism and Privacy Rights in the United States	33
Three	The Middle East and Africa	61
Four	Europe	77
Five	Northern and Southern Neighbors	119
Six	South America	129
Seven	Australia, New Zealand, and Asia	137
	Conclusion	155
	<i>Appendixes</i>	159
	<i>Notes</i>	179
	<i>Selected References</i>	213
	<i>Index</i>	221

Preface

Sadly, terrorism is far from a new phenomenon. While the attacks of 9/11 caused many in America who had previously given very little thought to the subject of terrorism to become increasingly focused upon the issue, the reality is that terrorism has been a feature of society for centuries. In fact, the word “terrorism” is believed to have originated back sometime between 1793 and 1794 during the French Revolution’s “Reign of Terror” when Robespierre’s Jacobins was reported to have executed more than 12,000 people who were deemed to be enemies of the Revolution. Robespierre was unapologetic about the use of terrorism as a means of achieving political goals and is reported to have said about his actions: “Terror is nothing but justice, prompt, severe and inflexible.”¹

Since its origins, various societies have had to deal with the plague of terrorism. Although specific types and phases of terrorism have arisen for a multitude of reasons, the essential challenge for societies confronting such threats has remained the same: that is finding a means to an end to the scourge of terrorism, while preserving the essential liberties and freedoms upon which modern democratic societies have been based.

Terrorism is not a recent creation; however, it is also undeniable that the current terrorist threat presents new and special challenges to our society. Indeed, the recent wave of terrorist activity has been particularly damaging and profound. The effects of the terrorism of the past few years have transformed and will long continue to influence the way we live for decades, if not centuries, to come. While many of these changes have occurred as a direct result of the acts of terrorists themselves, others have followed and will continue to grow out of our collective response to the acts of the terrorists.

History demonstrates adequately that caution must be exercised before undertaking a reactionary response to a new threat. Still, evidence suggests that all around

the world governments have been responding in a very rapid and extremely overbroad manner to the current perceived risk. Consider, for instance, the singular but incredibly significant example of the Patriot Act, fully titled, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). This very lengthy and extraordinarily detailed legislation was passed on October 26, 2001, only six short weeks after the terrorist attacks that devastated the country. The text of the USA PATRIOT Act exceeds 100 pages, making it the longest piece of emergency legislation passed in the shortest period, in all U.S. history. Such a rapid and utterly transformative response is sufficient cause to sound the alarm bells.

After the terrorist attacks, there was much speculation that many of the measures undertaken would be temporary in nature. However, all indications are that governmental powers continue to increase and expand in ways many of us never imagined would be possible just a few short years ago, while personal privacy rights and individual liberties continue to diminish. Now, more than five years after the attacks that devastated the country, it is time to take a step back and analyze whether the measures that have been taken in an effort to protect the country have truly been in the nation's best interest. If proper care is not taken and due consideration is not given now, it is more likely than not that the changes caused by our collective response to the terrorist acts will be largely negative.

In light of the foregoing, this book shall explore how the ongoing global war on terror has led to a global war on privacy. *Introduction* will introduce preliminary evidence supporting the notion that the war on terror has resulted in a war on privacy. It will examine the ways in which, led by the United States, various governments around the world have been responding to the threat of terrorism and will show how these responses have been eroding well-established privacy rights and individual liberties.

Chapter 1 will present a general overview of privacy rights in the United States before and immediately following September 11. Specifically, the chapter will present an in-depth examination of the trends in privacy regulation as they existed before September 11, 2001. The chapter will demonstrate how various factors, including the advent of new technologies, were leading to the enactment and enforcement of more stringent legislation concerning individual privacy rights. This chapter will explore some of the most prominent privacy rights laws that were passed in the United States during the 1990s and early 2000s. It will then show the general trends in privacy rights that had begun to develop just after September 11, 2001.

Having introduced the privacy regime, as it existed in the United States before September 11, Chapter 2 will move on to examining how the events of September 11 (and the legislation passed as a result thereof) have resulted in a startling and

significant erosion of privacy rights in the United States. Significant focus will be placed on the USA PATRIOT Act and similar legislation. This chapter will also highlight the government's data mining efforts and, in doing so, will show how corporations, educational institutions, and other private entities have been drafted into becoming foot soldiers in the government's war on privacy. Such draft has, of course, put many such entities in the impossible position of having to choose between responding to governmental demands for information on the one hand and honoring privacy commitments made to individuals and complying with privacy laws on the other.

Then, in Chapter 3 the discussion will shift to an analysis of privacy rights in the Middle East and Africa and will examine how such nascent rights have also been impacted by the global war on terror. While neither privacy rights nor Internet usage was very well developed before the attacks on America, generally in most countries in the region the slow march toward enhanced privacy protections was stalled considerably by the attacks against America and the governmental response that followed.

Chapter 4 will examine the impact that the war on terrorism had on privacy rights in Europe, with a particular focus on countries that are members of the European Union (EU). Privacy rights have long been respected in the Europe. In fact, in many European countries, privacy is considered as a fundamental human right. Member states of the EU have to implement in their local laws the requirements of the Data Protection Directive, a very comprehensive legislation that provides individuals with comprehensive privacy rights and places restrictions on the export of personal data outside the EU. At the same time, however, European countries have been battling terrorism for many years, and in the wake of the September 11 terrorist attacks against the United States and those that followed in United Kingdom, many European jurisdictions demonstrated a willingness to adopt tough new anti-terror measures, many of which had a palpable negative impact on privacy rights. The horrendous transit bombings that followed in Madrid and London only strengthened the resolve of many European countries to take all actions deemed necessary to reduce the likelihood of future terrorist attacks.

Chapter 5 will focus on our northern and southern neighbors: Canada and Mexico. As an important trading partner and close neighbor of the United States, Canada has been particularly impacted by US efforts to combat terrorism. Like the EU, Canada has comprehensive privacy legislation, enacted in advance of the 2001 attacks. Therefore, Canada has been trying to balance the need to collect, disclose, and use personal data with the need to protect the privacy rights of its citizenry. Mexico, as well, has been impacted in a dramatic way by the U.S.-led war on terror. Mexico has become a higher priority for law enforcement because of a growing

concern about the porous southern border and the potential for terrorists and/or dangerous materials to be smuggled into the United States.

Chapter 6 will focus upon Latin and South America. Privacy rights were somewhat slow in coming to the region of South America. Even today, there are many countries in South America that have not enacted any privacy laws and do not provide any constitutional protections to privacy rights. Nonetheless, in the late 1990s, a handful of South American countries did begin to consider and enact privacy and data protection laws. It is likely that such efforts were encouraged at least, in part, by the enactment of the European Data Protection Directive, which prohibits the export of personal data from the EU to third countries that do not provide adequate protection to personal data. For the most part, efforts to enact new privacy laws and strengthen existing legislation were diminished by the war on terrorism. At the same time, local governments found that they had a very clear basis for strengthening a wide range of anti-terror measures.

In Chapter 7, attention will shift to examining the privacy rights in the South Pacific and Asia. This chapter will demonstrate how the war on terrorism has been having a very negative impact on the privacy rights in many countries of the region. Like in many other regions examined in this book, privacy rights were largely under development at the time of the terrorist attacks in the United States. The growth and development of these privacy laws took an about-face in the wake of the terrorist attacks and in response to increasing demands for information from the U.S. and other governments. At the same time, many countries in the region engaged in increased surveillance and enacted various anti-terror measures, all of which had a negative impact on privacy rights.

The final chapter will argue that the erosion of privacy rights on a worldwide basis is fundamentally detrimental to a democratic society. While it is clear that efforts to prevent terrorism are essential, it is the position of this publication that such efforts can be carried out with greater respect for individual privacy rights. This chapter will also demonstrate why aggressively pursuing efforts to prevent terrorism and apprehend terrorists with little regard for privacy rights and civil liberties will lead to far-reaching negative consequences on a worldwide basis.

ACKNOWLEDGMENTS

I gratefully appreciate the research assistance of Dale Fulton, Haseeb A. Chowdry, and Elizabeth Weill-Greenberg, the secretarial support and laughter of Edwina Battle, and the encouragement of my supportive and highly talented colleagues at Goodwin Procter, LLP, including, most notably, Steven G. Charkoudian.

Introduction

OVERVIEW

Privacy is a relatively new concept. While it is true that today most jurisdictions around the world recognize privacy in some respect, the right to privacy, particularly as an enforceable legal right, is a relatively new creation. Moreover, there continue to be tremendous differences in how privacy is viewed, let alone how and even if, individuals may enforce their privacy rights. In certain jurisdictions, including most European countries, privacy is viewed as a fundamental human right. In other jurisdictions, especially the United States, the right to privacy is more often conceptualized as the right to be left alone from interference. Still, in other areas, including many Middle Eastern and some Asian countries, “privacy” in terms of commonly accepted Western conceptions is not often viewed as a matter of significant concern.

Generally, in most industrialized, Western nations, privacy rights developed slowly but somewhat steadily, at least until the latter part of the twentieth century. During the mid-to-late 1990s, privacy rights became the subject of increased focus and concern. One significant reason for this new focus was the advent of new technologies. Throughout this period, new technological developments were having a profound impact on the way in which we worked, played, and lived. They were enhancing our ability to exchange information, content, and data rapidly and across vast distances and national boundaries. Efforts to collect, process, and mine data, which were once extraordinarily time-consuming processes, could suddenly be accomplished almost instantaneously. As a result, there was increasing concern about how such technologies might have an adverse impact upon individual privacy rights. In essence, we wondered how to preserve this vague right to be left alone from interference, as the new technologies made it less and less likely that we would indeed be left alone.

Around the same period, a comprehensive data protection regime with elements of extraterritoriality was just coming into force in Europe. Europe’s main

data protection directive¹ (the Data Protection Directive), which was passed in 1995 and took effect in 1998, severely limited the ability of enterprises and organizations to transfer any personal data outside the European Economic Area (EEA) unless the country to which the data would be transferred provided *adequate* protection to such personal data. As a result, many jurisdictions were compelled to implement new privacy and data protection laws so as to ensure that entities within their national boundaries would be able to continue to receive personal data from within the EEA. The United States, of course, opted for a different approach and undertook efforts to negotiate a self-regulatory scheme as an alternative to comprehensive data privacy legislation.

All of the foregoing factors contributed to an increased demand for comprehensive privacy laws. And many jurisdictions responded. During this period, around the globe, many privacy laws were introduced and/or enacted.² At the same time, governmental and regulatory authorities in various jurisdictions directed attention toward launching investigations and commencing enforcement actions against companies that had been viewed as violating individual privacy rights.³

Back then, it seemed that, despite the lobbying efforts of some businesses, efforts to ensure the protection of individual privacy rights would only continue to grow and strengthen. There was even speculation that the United States would perhaps enact a broad, general federal privacy law, not too dissimilar from that of the EU data protection directive.

Then came the unspeakable and unexpected events of September 11—along with the additional attacks that were to follow. The terrorist attacks of September 11, 2001 were tragic, horrific events that changed the course of history on so many levels. While an in-depth analysis of all of the effects and repercussions of the terrorists attacks is clearly beyond the scope of this publication, this book will seek to examine one very significant side-effect of the attacks, that is, the general erosion of individual privacy rights in the United States and across the entire globe that accompanied the war against terrorism that followed 9/11. At the very least, the preoccupation with fighting terrorism and preventing the next terrorist attack reduced the focus on and concerns about individual privacy rights. Arguably, as this book will contend, the war on terror not only stalled the further advancement of privacy rights, but caused degradation in individual privacy rights in many different areas and on many different levels.

INITIAL RESPONSE TO THE TERRORIST ATTACKS OF 9/11

The attacks on America led to shock and horror around the world. World leaders responded immediately, expressing their collective outrage at the attacks, while extending their condolences and offers of assistance.⁴ Likewise, citizens from all

over the world expressed their sorrow, grief and solidarity with the United States. Not too long after this initial reaction, governments across the globe began to contemplate and eventually implement measures that they believed would be needed to prevent future tragedies from occurring anywhere in the world.

Still reeling from the horrific attacks and eager to prevent the occurrence of similar—or even worse—tragedies in the future, American legislators rushed to adopt and implement legal measures to prevent terrorism and capture terrorists. Given the nature of the current wave of terrorism and, specifically, the fact that many terrorists are organized in sleeper cells, striving to blend into society until it is time to attack, many of these measures included elements of enhanced powers of surveillance and investigation. At the time, it was maintained that many of these measures would be, in effect, temporary. But, now, more than five years after 9/11, all indications suggest that surveillance activity is still increasing, while efforts to protect privacy continue to decline.⁵ In fact, it seems that each day brings more news reports revealing additional ways that the government has been infringing upon individual privacy rights in its “War on Terror.”

The profound changes in privacy regulation were not limited to the United States. Since 2001, the privacy landscape has shifted enormously in many, if not most, countries around the world. The motivations behind such changes are varied, including pressure by and/or incentives from the United States government or other governments, the demands of their own citizens, and/or a concern about preventing horrific terrorist attacks from occurring within their own boundaries. Whatever the reasons may be, many countries have implemented legislative changes that are dramatically affecting the overall level of privacy enjoyed by their citizens.

A Rush to New Legislation

In the immediate aftermath of the September 11 attacks, international organizations responded swiftly, demanding that national governments undertake increased efforts to fight terror. Just a day after the attacks, the United Nations adopted Resolution 1368, calling on increased cooperation between countries to prevent and suppress terrorism.⁶ Then on September 28, 2001, the United Nations Security Council adopted the more significant Resolution 1373.⁷ Through this resolution, the Security Council called upon all States to take a very wide range of measures to fight terrorism. Specifically, UN member states were instructed to do the following:

- criminalize the willful provision or collection of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, to carry out terrorist acts;

- freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting for, or at the direction of, such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;
- prohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources, or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons, and of persons and entities acting for or at the direction of such persons;
- refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists;
- take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information;
- deny safe haven to those who finance, plan, support, or commit terrorist acts or provide safe havens;
- prevent those who finance, plan, facilitate, or commit terrorist acts from using their various territories for those purposes against other States or their citizens;
- ensure that any person who participates in the financing, planning, preparation, or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that, in addition to any other measures against them, such terrorist acts are established as serious criminal offences in domestic laws and regulations and that the punishment duly reflects the seriousness of such terrorist acts;
- afford one another the greatest measure of assistance with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings;
- prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery, or fraudulent use of identity papers and travel documents;

- find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives, or sensitive materials; use of communication technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups;
- exchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts;
- cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts;
- become parties as soon as possible to the relevant international conventions and protocols relating to terrorism, including the International Convention for the Suppression of the Financing of Terrorism of December 9, 1999;
- increase cooperation and fully implement the relevant international conventions and protocols relating to terrorism and Security Council resolutions 1269 (1999) and 1368 (2001);
- take appropriate measures in conformity with the relevant provisions of national and international law, including international standards of human rights, before granting refugee status, for ensuring that the asylum seeker has not planned, facilitated, or participated in the commission of terrorist acts;
- ensure, in conformity with international law, that refugee status is not abused by the perpetrators, organizers, or facilitators of terrorist acts and that claims of political motivation are not recognized as grounds for refusing requests for the extradition of alleged terrorists.

Resolution 1373 was adopted under chapter VII of the United Nations Charter, since the Security Council determined that the attacks of September 11 were deemed to constitute “a threat to international peace and security.”⁸ Under the United Nations Charter, the Security Council is empowered to direct member states to comply with the program it has adopted, rather than merely suggesting or recommending courses of action.⁹

While the suggested United Nations program certainly seems to have been based on proper motivations, when one looks back in retrospect at the terms of the resolution, two issues are of particular concern. First, the resolution failed to include any

precise definition of terrorism. Although it is true that it can be very difficult for a diverse group of parties to come to terms with a precise definition of terrorism, further efforts should have been directed toward this goal at the time the resolution was being adopted. When “terrorism” as a crime is defined without proper precision, there will be the risk that the actions of ordinary criminals—or, even worse, political protesters—will be considered terrorism, and result in subjecting the perpetrators of such acts to the harsh punishments that would apply under law to perpetrators of “terrorism.” Subsequent chapters that examine the various national measures that have been adopted around the world will show how the lack of precision in defining terrorism can be a very serious problem.

A second major concern regarding Resolution 1373 is that it failed to require member states to address human rights considerations when implementing measures to counter the threat of terrorism. The subsequent discussion regarding national measures that have been adopted against terrorism will show that many laws and policies that have been adopted in the wake of September 11 infringe upon individual rights generally and privacy rights specifically. While it would not have avoided the problem entirely, it would have been useful if the Security Council resolution had required member states to include privacy and other human rights considerations in their counterterrorism initiatives. If nothing else, at the very least, doing so may have caused some leaders and legislators to keep such considerations in mind when developing their counterterrorism response.

The passage of Resolution 1373 appears to have been influential in motivating UN member states to modify their national laws to respond to the threat of terrorism. The UN Counter-Terrorism Committee maintains Web pages devoted to the national response to Resolution 1373, and the reports contained therein detail a lot of the responses that have been undertaken to date.¹⁰ Even a cursory review of such pages demonstrates that countries have been taking the mandate put forth by the UN Security Council very seriously. While it is clearly beyond the scope of this publication to examine all of these measures in detail, the sheer volume of the measures proposed worldwide in the immediate aftermath of the attacks is certainly worth noting.

Of course, the immediate international response was not limited to the United Nations. Other international and regional organizations also responded quite rapidly. The Council of Europe condemned the attacks, urged solidarity among nations, and called upon national governments to cooperate more with other governments in efforts to prevent, investigate, and prosecute criminal matters.¹¹ About two weeks after the attacks, the Council of Europe Parliamentary Assembly asked countries to ratify conventions combating terrorism, lift any reservations in

these agreements and extend the mandate of police working groups to include focus on “terrorist messages and the decoding thereof.”¹² Such initial statements foreshadowed the more concrete and developed efforts to fight terror that would soon follow in many countries around the world.

In the weeks and months after the attacks and the immediate initial reaction thereto, many jurisdictions took concrete efforts to expand and enhance surveillance and investigative powers. A number of countries followed the directions of the Council of Europe and ratified international instruments, and numerous countries passed new laws to increase the ability of authorities to conduct communications surveillance. A great number of jurisdictions also increased search and seizure powers and expanded the ability of law enforcement authorities to detain suspects.

Unofficial actions of many governments also impacted privacy laws that had already been enacted prior to the 2001 attacks. For example, many of the privacy laws that were enacted prior to September 11, particularly those in Europe, had included comprehensive data subject access rights. However, the overall decline in privacy rights that occurred after the terrorist attacks also impacted this aspect of privacy rights. Justified by a need to ensure the protection of sensitive intelligence data, subject access requests are restricted as some databases are being exempted from both data protection and freedom of information laws.

The effects of the terrorist attacks on privacy have been profound and widespread. Not only have governments adopted measures to increase and enhance their surveillance and investigatory powers, in the wake of the terrorist attacks many governments have found increased support and new justification for continued study or even adoption of proposals for measures that had previously had little support (such as national identity cards). In many countries, legislative measures adopted to fight “terrorism” were drafted so broadly so as to permit an interpretation that would restrict virtually any kind of dissent.¹³

The general focus on the need to prevent terrorism has empowered police and judicial authorities to take actions that may have been deemed questionable before the terrorist attacks, for example, requiring the removal of veils for driver’s license photographs,¹⁴ placing restrictions on trainspotters and photographers¹⁵ in a wide range of circumstances, and requiring law school administrators to turn over attendee lists from legal conferences concerning Islamic issues.¹⁶ While in many cases such efforts may not have been motivated solely by concerns about terrorism, it has become much easier to establish a connection—either expressly or impliedly—between such efforts and the general war on terror.

Of course, upon initial consideration, preventing a hobbyist from viewing and photographing a train may not seem to be of great concern, especially if doing so may help prevent a terrorist attack against a train. However, all of these restrictions must

be evaluated both in and of themselves and also in their totality. Such restrictions can have a chilling effect on all kinds of behaviors, as people become increasingly fearful of the prospects of being punished for engaging in ordinary behavior. And when taken in sum, such limitations detract people from the general culture of freedom and liberty upon which this country was based.

September 11 as a Rationale for Clamping Down on All “Terrorists” Worldwide

When examining the global impact of the war on terror, it is impossible to ignore the fact that around the world, governments have been using the September 11 attacks, as the resulting response thereto, as a rationale for enacting measures targeted at matters of particular concern to them within their own national boundaries. Various governments have become willing participants in the global war on terror, and some have used such participation as a means for equating separatists or other groups with political claims with the kinds of terrorists associated with the September 11 attacks on the United States. This phenomenon has been observed by a number of human rights groups and other organizations; for instance, a recent report published by Human Rights Watch substantiates this claim, contending that “[m]any countries—Uzbekistan, Russia and China among them—used the “war on terrorism” to attack their political opponents, branding them as Islamic terrorists.”¹⁷

The strongest example of this phenomenon, some may argue, may be Russia’s attempts to clamp down on Chechen rebels. Some have contended that Russia has used the 9/11 attacks to bolster its own internal counterterrorism measures and to urge the United States to support and even participate in Russia’s struggle against its own terrorists.¹⁸

Another example some may say may be witnessed in the Turkish government’s increased efforts to control the political activities of the Kurdistan Workers’ Party (PKK). Reports have suggested that the global war on terror has helped the government in Ankara in its struggle against the PKK, in that the global battle against al-Qaeda-type terrorists has helped create an environment that is inhospitable to all groups classified as terrorists by their own local governments.¹⁹

Arguably, similar activities have been occurring in Colombia as it struggles against various guerilla groups. Indeed, Colombian President Álvaro Uribe Vélez has not been timid in his attempts to link the global war on terror to the country’s own internal struggles.

In his inauguration speech, for example, Uribe used terrorism to refer to “any violence against [a democratic state]”. As the US prepared to invade Iraq and

remove Saddam Hussein from power, the president added Colombia to the coalition of the willing”—the only South American nation to join—and explicitly linked Colombian violence to events in the Middle East.²⁰

There have also been claims that “Chinese authorities now call the separatists in the western province of Xinjiang ‘terrorists’ to justify repression and shutting down publications.”²¹ Clearly, there is cause for great concern when these kinds of “side effects” of the U.S.-initiated war on terror are being felt worldwide.

Increased Information Sharing between Private Companies and the Government

Because of the global war on terror, there has also been a dramatic increase in information sharing between private entities and the government. In the United States, such information sharing has occurred within a number of industrial sectors, but the activity within the travel and communications sectors has been particularly heavy. There have been numerous reports of telecommunication companies and airlines sharing customer data and information with various governmental bodies, often in contravention of applicable privacy laws and the privacy promise they have made to their customers and almost always without advance notice to their customers.

Recent reports have emerged that during 2005 the Federal Bureau of Investigation (FBI) secretly sought information on more than “3,501 American citizens and legal residents from their banks and credit card, telephone and Internet companies without a court’s approval.”²² Not long ago, dramatic reports of a comprehensive program to spy into Americans’ telephone calling data have emerged and even more recently, details of a comprehensive data sharing program between educational institutions and the FBI came to light. Many experts feel that this is one of the most significant privacy issues of the future. Private companies have been able to amass huge amounts of data regarding individuals’ purchasing habits, communications, travel, social networks, work history, finances, and more. Increasingly, the government may be looking to access, combine, mine, and otherwise process data from these databases concerning various initiatives, including its efforts to prevent future terrorist acts.

Against this backdrop, across the board and around the world, there has been a corresponding decline in efforts to protect privacy on the commercial side. With governments and individual citizens concerned about terrorism and focused on measures to prevent the same, efforts to place limitations on the ability of online retailers to use personal data for marketing purposes suddenly seemed less significant

to legislators and regulators. This is ironic because evidence from around the world suggests that consumers remain concerned about the privacy and security of their online activities, especially given the slew of very public data breaches occurring in the United States and elsewhere throughout 2005 and 2006. Consider, for instance, a May 2006 global survey conducted by the UN International Telecommunication Union, which showed 44 percent of respondents claiming that privacy is poorly respected online and a startling 64 percent of respondents claiming that they avoided certain online activities because of security concerns.²³ Moreover, an April 2006 survey of 1,150 adults in the United States found that only 18 percent believed that existing laws are sufficient to protect them on the Internet.²⁴

Furthermore, recognizing that many commercial entities have much valuable information concerning individuals, the governments of the United States and other countries have also exerted pressure on private industry, demanding the companies in the private sector to share certain information with the government. As noted above, this has been most visible in the travel industry. The governments of many countries, including, without limitation, the United Kingdom²⁵ and Canada,²⁶ have made proposals for increased sharing of airline passenger data with the government. Still, while widespread in the travel industry, such proposals for increased information sharing have not been limited to this industry. Clearly, there has been a dramatic increase in information sharing between financial institutions and governments.²⁷ Even charitable organizations have not been immune to such demands as governments increasingly examine charitable donations to investigate potential terrorist ties.

RISING CONCERNS

The various horrific terrorist attacks that have occurred during the past few years are still very fresh in the minds of most individuals. Many people remain of the view that the government should do everything within its power to prevent another possible terrorist attack, and they are comfortable with the notion that privacy rights and individual liberties will take a back seat to these efforts. At the same time, however, there is a rising chorus of voices that are beginning to call for greater focus on efforts to protect privacy rights. Such voices are beginning to clamor for more restraint and are calling upon the government to be more strategic and targeted concerning its data collection and data-mining efforts.

Survey results offer support for the notion that, slowly but surely, public concern over privacy rights within the context of the fight against terrorism is on the rise. In the time that immediately followed the terrorist attacks, many surveys demonstrated a high level of tolerance for privacy invasions, provided that such