INTRODUCTION

Securing the Freedom of the Communications Revolution

Michael K. Powell*

At the dawn of the American Revolution, Thomas Paine wrote that "the design and end of government" was to provide the public with "freedom and security."[1] For the past 200 years, Americans seldom have had to ponder or grapple with the potential contradiction between these two goals because the contradiction emerges most palpably only during times of national crisis. Events like President Lincoln's suspension of habeas corpus, President Roosevelt's internment of Japanese-Americans, and President Nixon's attempted suppression of the *New York Times'* publication of the *Pentagon Papers* underscore the tension between these two principles, as well as the dangers of pursuing one goal at the expense of the other. As Thomas Paine so clearly understood, we must strike the appropriate balance between freedom and security if we are to maintain our American values and way of life during times of national crisis.

As with so many other things in our lives, our perception of the relative roles of freedom and security changed forever on September 11, 2001 ("9/11"). On that day we were indelibly reminded that freedom is not free, that it cannot exist in a vacuum, and that enhanced security is the price we

* Michael K. Powell served as Chairman of the Federal Communications Commission ("FCC") from January 22, 2001, until March 18, 2005. Prior to being designated Chairman by President George W. Bush, Mr. Powell served as a Commissioner since 1997. Mr. Powell wishes to thank Shannon Lipp, Gregory Cooke, and Pete Belvin for their invaluable assistance with this article.

1. THOMAS PAINE, COMMON SENSE (1776), *reprinted in* COLLECTED WRITINGS 8–9 (Eric Foner ed., 1995).

must pay to preserve it. That day required us to recalibrate the delicate balance between freedom and security. For us in the communications industry, this recalibration is particularly difficult because we must balance the promise of new modern digital technologies that provide global communication with the security concerns, both public and private, based on those transmissions.

Today, freedom—in the form of the free exchange of ideas, open and competitive markets, and technological innovation—is fueling an ongoing revolution in the communications industry. As a result, the telecommunications sector has emerged as the driving force of both the American economy and the global marketplace, with consumers reaping the benefits. But we are only at the threshold of this revolution: a digital future awaits where competitive markets, open broadband networks, and cutting-edge services will fundamentally alter every aspect of our lives.

The challenge we face, therefore, is twofold. First, we must understand how current law and regulation strike a balance between freedom and security in the local, national, and international environments in which the telecommunications industry functions. As the articles in this issue illustrate, the complexities of telecommunications technology and economics combine with multiple sources of governmental involvement to weave an intricate pattern of rights and responsibilities. It is only when these complexities are better understood that we can face the second challenge of assessing whether the balance between freedom and security reflected in current law is proportionate, or needs further refinement.

The stakes involved in accurately striking this balance cannot be overestimated. Shall we turn our backs on almost a quarter century of open market progress to shield ourselves from future threats? Shall we hobble the Internet because of its vulnerabilities? Shall we close our competitive markets because they are impossible to control or predict? Shall we limit new participants' ability to offer innovative services because we cannot forecast all the ways in which such services may be used? The answer to all of these questions is a resounding no. Security need not, and does not, require us to reject freedom, but it *does* require us to take a hard look at the post-9/11 world and compels us to find a balance that enhances both. The Federal Communications Commission ("FCC") has been engaged in this balancing effort ever since 9/11. An abbreviated description of these efforts demonstrates just how extensive the reassessment process needs to be, involving not just the FCC's rules, but its fundamental organization as well.

In November 2001, the FCC began restructuring its internal operations to conform to post-9/11 security-related concerns. As our first step, we created an internal working group called the Homeland Security Policy

Council ("HSPC"), comprised of senior management from each of the Bureaus and Offices.[2] The HSPC works with the communications industry and representatives from federal, state, local, and tribal governments to develop and coordinate the FCC's homeland security initiatives. This was followed in July 2003 by the creation of an internal Office of Homeland Security to support the HSPC and the FCC by providing intra- and interagency coordination on the homeland security aspects of all FCC matters.

Restructuring the FCC by integrating homeland security into its mission has in turn enabled the agency to work closely with industry to formulate policies that successfully balance freedom and security. These public-private partnerships have encouraged both industry and government to find common ground, and have led to the implementation of a series of initiatives that augment the capabilities of our nation's first responders to deal effectively and safely with threats to life and property. For example, the 800 MHz proceeding achieved a solution to the interference problems in first responder radio communications;[3] the 4.9 GHz proceeding assisted public safety scene management, and dispatch and vehicular operations by accommodating the use of a variety of new broadband applications such as high-speed digital technologies and wireless local area networks;[4] the Intelligent Transportation Systems proceeding advanced benefits such as the ability to monitor traffic from a control point and to route first responders along the path of least resistance;[5] and the Wireless Enhanced 911 proceeding produced a schedule for phasing in the most advanced wireless-based location and lifesaving technologies.[6] In each proceeding, the close cooperation of industry was essential to its success.

2. Linda Blair, Deputy Chief of the Enforcement Bureau, deserves special thanks for her leadership as Deputy Director of the HSPC since its inception.

3. *See* Improving Public Safety Communications in the 800 MHz Band, *Report and Order, Fifth Report and Order, Fourth Memorandum Opinion and Order*, 19 F.C.C.R. 14,969 (2004), *as amended by Erratum*, 19 F.C.C.R. 19,651 (2004), *and by Erratum*, 19 F.C.C.R. 21,818 (2004).

4. *See* The 4.9 GHz Band Transferred from Federal Government Use, *Memorandum Opinion and Order and Third Report and Order*, 18 F.C.C.R. 9152 (2003), *stay granted by* The 4.9 GHz Band Transferred from Federal Government Use, *Order*, 19 F.C.C.R. 15,270 (2004), *and reconsidered in part by* The 4.9 GHz Band Transferred from Federal Government Use, *Memorandum Opinion and Order*, 19 F.C.C.R. 22,325 (2004).

5. *See* Amendment of the Commission's Rules Regarding Dedicated Short-Range Communications Services in the 5.850-5.925 GHz band (5.9 GHz band), *Report and Order*, 19 F.C.C.R. 2458 (2004). Intelligent Transportation Systems ("ITS") or Dedicated Short Range Communications ("DSRC") systems operate in the 5.850-5.925 GHz band.

6. *See* Revision of the Commission's Rules to Ensure Compatibility With Enhanced 911 Emergency Calling Systems, *Report and Order and Further Notice of Proposed Rulemaking*, 11 F.C.C.R. 18,676 (1996). *See also* IP-enabled Services, *Notice of Proposed Rulemaking*, 19 F.C.C.R. 4863 (2004).

Restructuring has also led to increased interagency coordination . The FCC currently is working closely with the Department of Homeland Security, the National Telecommunications and Information Administration, and other federal, state, and regional emergency response providers to implement provisions from the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004[7] regarding the efficient use of broadband and wireless spectrum for emergency response providers.[8] In an ongoing effort, the FCC is working in close cooperation with law enforcement to ensure that emerging technologies are compatible with law enforcement's need to conduct electronic surveillance to protect the public from criminal activity. The Communications Assistance for Law Enforcement Act of 1994 ("CALEA")[9] requires telecommunications carriers to have the necessary capability and sufficient capacity to assist law enforcement regardless of their specific systems or services. As a result, the FCC is currently addressing issues regarding the application of CALEA to emerging technologies such as Voice over Internet Protocol and other IP-enabled services.[10]

By establishing a number of government-industry forums, the FCC has been able to help competitors voluntarily agree on common approaches to security issues. In fact, some of the most successful FCC efforts have not required rulemakings at all. Rather, these forums have encouraged industry to adopt and implement voluntary best practices to improve their operational security in a manner that directs the energies of the competitive marketplace to meet both the vulnerabilities as well as the opportunities of new technologies and the increasingly competitive global marketplace.

For example, in 2002, the FCC rechartered one such forum, the Network Reliability and Interoperability Council ("NRIC"), to focus on continuity of operations and restoration of service in the event of terrorist attacks or natural disasters, and again rechartered NRIC in 2004 to consider end-to-end reliability and interoperability of emergency services and networks—especially newer wireless networks.[11] To date, the carriers, manu-

7. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004) (to be codified at scattered sections U.S.C.).

8. *Id.* §§ 7501, 7502(a).

9. Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 47 U.S.C. §§ 1001–1021 (2002)).

10. *See* Communications Assistance for Law Enforcement Act and Broadband Access and Services, *Notice of Proposed Rulemaking and Declaratory Ruling*, 19 F.C.C.R. 15,676 (2004); IP-enabled Services, *Notice of Proposed Rulemaking*, 19 F.C.C.R. 4863, para. 50 n.158 (2004) (explaining that the FCC intends to coordinate its efforts in both the instant docket and the CALEA rulemaking docket).

11. *See* NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL, CHARTER OF THE NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL - CHARTER VII (Apr. 15, 2004) *available at* http://www.nric.org/charter_vii/NRICVII_Charter_FINAL_Amended_2004_

facturers, and their government colleagues who comprise NRIC have produced over 800 industry best practices that focus on critical components such as physical security, cybersecurity, business continuity and disaster recovery, and public safety. Similarly, in March 2002, the FCC chartered the Media Security and Reliability Council ("MSRC") to develop best practices designed to assure the optimal reliability, robustness, and security of broadcast and multichannel video programming providers.[12] MSRC produced 100 best practices for media companies to adopt, covering such diverse topics as local coordination and planning, emergency procedures, the Emergency Alert System, vulnerability assessments, disaster recovery plans, physical security, and redundant facilities.

Despite the complexities of technology, the myriad assortment of principals and the range of perspectives on the issues, these government-industry partnerships succeed for one basic reason: these partnerships motivate participants to find common ground towards securing our nation's communications infrastructure by harnessing the same energies that drive competition.

And in these efforts I find tremendous hope. For they tell us that, notwithstanding the complexities of the matters at hand and the inevitable philosophical, economic, and technical differences that occur between and among different government agencies and competing segments of the telecommunications sector, it remains possible to reasonably balance the competing interests of freedom and security. This balancing may not be easy and at times it may not be perfect—but it is at least *possible*. This issue of the *Federal Communications Law Journal* provides a thoughtful contribution to this ongoing process by making us think about how the balance is currently struck and how we may perhaps improve it in the future.

3_12_04.pdf.

12. *See* MEDIA SECURITY AND RELIABILITY COUNCIL, CHARTER OF THE MEDIA SECURITY AND RELIABILITY COUNCIL (Mar. 26, 2002) *available at* http://www.mediasecurity.org/members/msrccharter.html.