

FOREWORD

Communications Policy for the Next Four Years

Senator Conrad Burns*

I.	ENSURING INFORMATION SECURITY IN A DIGITAL WORLD	168
II.	SPIES AMONG US	169
III.	NEXT-GENERATION E-911.....	170
IV.	SPAM	170
V.	TV RATINGS FAIRNESS	170
VI.	ICANN REFORM	171
VII.	DIGITAL DEMOCRACY	171
VIII.	BROADBAND DEPLOYMENT	172
IX.	UNIVERSAL SERVICE REFORM.....	172
X.	SPECTRUM REFORM	172

With the second Bush Administration already underway and the resignation of Chairman Powell on the horizon, communications policy is at the forefront of current debate. Recognizing the nature of this discourse, the time seemed right for the *Federal Communications Law Journal* to create a forum for evaluation and analysis of the current and future issues in communications law. The Authors of the pieces in this issue bring differing perspectives to the discussion, and I also offer my own hopes for the next four years as well.

* Conrad Burns is the longest-serving Republican senator in Montana history; Chairman of the Subcommittee on Communications of the Senate Committee on Commerce, Science and Transportation.

We are in a digital age. It is no longer a world where we can distinguish between voice, video, and data. Everything now is in the indistinguishable form of ones and zeroes. This will pose new challenges as we continue forward with reform legislation.

We are in an age where the Internet and telecom industries are at a crossroads. In this era of consolidation, terrorism, and rapid technological innovation, we need to protect consumers, strengthen information security, and usher in reform for twenty-first century communications. In the Senate, we have been working on these goals for some time now, including spyware, spectrum reform, E-911, ICANN reform, broadband expensing, wireless privacy, and universal service reform.

I. ENSURING INFORMATION SECURITY IN A DIGITAL WORLD

Goal: We must impose significant penalties on online theft of personally identifiable information or misrepresentation in support of such activity. We must mandate responsibilities on communications networks in support of enforcement. We must define limits on use of personally identifiable information collected by radio-frequency identification (“RFID”) devices.

As more and more economic activity migrates to the Internet, “phishing,” or illegal theft of personal information—such as Social Security numbers, bank account numbers, or passwords to secure sites—is a growing problem. Meaningful penalties are necessary to curb this activity, which can take place either via software (spyware) surreptitiously entered into a personal computer, or by misrepresentation via email or other means of open communications. We are looking into these practices to ensure that the proper authorities have the tools necessary to go after the offenders. To shift the balance of power away from the malicious code writers who seek to cause informational and financial damage, we must also support the private sector’s ongoing proactive attempts to mitigate remotely exploitable security vulnerabilities.

Although the proliferation of RFID devices has led to economic efficiencies and increased convenience to companies and individuals in many areas, there has not been enough attention paid to how the personal data collected and disseminated by RFID devices, and the networks that support them, is used. In many cases the potential for abuse exists, and we must raise awareness about how entities that collect and propagate personal data using these devices can be used.

II. SPIES AMONG US

Goal: We must specify conditions under which installation of software by a third party on private computers is permissible and impose civil and criminal penalties for unauthorized installation of certain types of software on private computers.

The secluded nook we once thought we had within our personal computers installed in the privacy of our own homes is quickly becoming a highly trafficked freeway where online moles bury their programs and even the most experienced users cannot always spot and remove the hidden and malicious spyware programs left behind. These programs pose serious security threats as they work invisibly to track and collect data about computer users.

Spyware refers to software that secretly collects information about computer users and shares it with others over the Internet without the users' knowledge or consent. Any legitimately downloaded program may act as a Trojan horse, carrying with it a variety of other spyware programs.

Spyware is often used to track the movements of consumers online or even to steal passwords, and the holes it punches in a computer's security may be difficult to close. As noted by an article in *PC Magazine*, while the file-sharing networks that often distribute spyware may be free in monetary terms, the costs to a user's privacy are steep. Of the 60 million users of one popular file-sharing program, few know they are being watched through the spyware that was downloaded onto their computers.

The depth—and hidden nature—of this problem is why we must continue to work to combat the flood of spyware casting a pall over the growing online population. The Software Principles Yielding Better Levels of Consumer Knowledge ("SPYBLOCK") Act relies on a common sense approach to prohibit the installation of software on consumers' computers without notice, consent, and reasonable uninstall procedures. The notice and consent approach that the SPYBLOCK Act takes would end the methods that some bad actors use to secretly download programs onto computers. It will force providers to give consumers clear and conspicuous notice that a software program will be downloaded to their computers and require user consent.

It is impossible to understand how any of the individuals or companies using spyware believe that tracking Internet usage, stealing passwords, and hijacking the processors of someone's computer, all without their knowledge, is justifiable. When surfing the Internet, everyone should have the privacy and security they expect.

III. NEXT-GENERATION E-911

Goal: We must secure funding for the Ensuring Needed Help Arrive Near Callers Employing 911 (“E-911”) joint program office so that grants are made available as outlined in the E-911 Act. We must also explore options to ensure that Voice over Internet Protocol (“VoIP”) services are able to provide E-911 services and identify future technologies that will integrate with today’s E-911 system in order to provide public safety and tools that can save lives.

With the advent of technologies like VoIP, users of this technology must have the same life-saving emergency communications services as those using landline and wireless phone services.

IV. SPAM

Goal: We must work with the executive branch to enforce the CAN-SPAM Act and more aggressively pursue email spammers.

Spam, or unsolicited commercial email, is an increasingly serious problem that threatens to clog the Internet with junk messages, undermining its utility as a global communications network. Recent estimates predict that spam will cost U.S. businesses up to \$90 billion in 2005.

The CAN-SPAM bill, signed into law by President Bush on December 16, 2003, requires senders of unsolicited commercial email to provide an easy unsubscribe option for consumers and imposes harsh penalties on transgressors who falsify information to mask the origins of the sender. We have seen a steady flow of enforcement in the past few months from ISPs as well as the Federal Trade Commission (“FTC”). This continued effort will send the clear message to spammers that the work they do is out of bounds. We must ensure that the FTC devotes the necessary resources to enforce CAN-SPAM, and continue to coordinate with parliamentarians and agencies overseas to battle this scourge of the digital age.

V. TV RATINGS FAIRNESS

Goal: We must ensure that TV ratings are accurate and fair to all segments of the population and explore the proper government role in maintaining the public interest in TV ratings.

Last year, there was much controversy over the introduction of Local People Meters (“LPMs”) by Nielsen, the monopoly TV ratings company. Although Nielsen, overseen by the Media Ratings Council (“MRC”), is taking steps to ensure that all demographic groups are counted fairly, there is still a significant degree of dissatisfaction in the industry with Nielsen’s

approach. The public interest in maintaining accurate and fair TV ratings remains clear, and we must continue to monitor the situation, in consultation with key players.

VI. ICANN REFORM

Goal: We must strengthen and secure the infrastructure of the Internet and ensure the Internet Corporation for Assigned Names and Numbers (“ICANN”) adheres to its mission. We must also examine the current U.S. government role in ICANN oversight.

ICANN is a nonprofit private company created by the Clinton Administration to manage the technical aspects of management of the domain name system (“DNS”), as well as the assignment of Internet numbers (IP addresses), for all Internet users. After a rocky start, ICANN has made strides in recent years toward developing an institutional framework appropriate to its mission. However, it continues to come under pressure to address other, nontechnical areas outside its charter and mandate. Politically driven international processes threaten to push Internet governance back to governments or international bureaucracies. In addition, the administration may allow the Commerce Department’s current oversight agreement with ICANN to expire in 2006, which would effectively end the U.S. government’s highly successful historic role as the chief sponsor and responsible steward of the Internet as a unitary global communications network.

VII. DIGITAL DEMOCRACY

Goal: We must leverage the Internet revolution to bring government to the people.

I held Congress’ first interactive, online hearing on June 12, 1996. Now, nine years later, we must make the legislative process available to citizens over the Internet through cybercasts and online documents.

The Digital Democracy Act is a good-government bill that requires that certain governmental proceedings and documents be made available via the Internet. Congressional proceedings and hearings, along with public executive branch meetings, should be available to the public in real time and archived along with searchable transcripts. Furthermore, Congressional Research Service (“CRS”) reports should be posted online for public use.

VIII. BROADBAND DEPLOYMENT

Goal: We must ensure that the benefits of the Internet reach even the most rural of our citizens.

Everyone should have access to the Internet. We must pass legislation to provide tax incentives to businesses that invest in broadband, with a focus on accelerating the deployment of high-speed Internet access across the country, especially in rural America. Currently proposed legislation creates a temporary tax incentive for providers in the form of “expensing,” allowing an immediate deduction of a capital expenditure in the first year of service rather than depreciating that investment over time.

In the case of current generation broadband investments in rural and underserved areas, this legislation would allow 50 percent expensing of the investment, with the rest to be depreciated according to normal depreciation schedules. When providers build out next generation broadband networks, which are typically more expensive, it provides for 100 percent expensing.

IX. UNIVERSAL SERVICE REFORM

Goal: We must ensure affordable telecommunications service to rural consumers.

We must continue to firmly support a solvent and stable universal service fund that sustains consumers in rural America through the availability of high-quality and affordable telecommunications service.

However, significant reforms to the universal service contribution system are needed for rural consumers. These initiatives must be guided by the following principles:

- (1) ensure the stability and sustainability of the universal service fund;
- (2) ensure that contributors are assessed in an equitable and nondiscriminatory manner;
- (3) minimize the regulatory costs associated with complying with universal service obligations; and
- (4) develop a contribution recovery process that is fair and readily understood by consumers.

X. SPECTRUM REFORM

Goal: We must transform an inefficient and burdensome framework into a more balanced model for consumers and businesses.

We must move away from the current auction model, under which the public’s airwaves are transferred to private users based on the highest

bidder. This policy has resulted in bankruptcies, botched auctions, and failed promises for consumers. We should examine a totally different approach based on a royalty or revenue-sharing concept. These kinds of models have worked well in several Asian countries, such as Hong Kong and Singapore, and balance the costs more fairly among consumer, government, and private operators.

174

FEDERAL COMMUNICATIONS LAW JOURNAL

[Vol. 57]