Chapter II

Less Safe:
The Dismantling of Public Information Systems after September 11

Harry Hammitt, Access Reports, Inc., USA

Abstract

Since the terrorist attacks of September 11, 2001, there has been a tightening of public access. In response to perceived security threats, government agencies have taken information down from Web sites, curtailed or restricted access to electronic sources of information, broadened the interpretation of FOIA exemptions, created or augmented new categories of restricted information, and prohibited public access for critical infrastructure information. These policy responses have been based both on the perceived security threat and an inhospitable attitude toward open government on the part of the Bush administration.
Introduction

By the end of the Clinton administration, government at all levels was becoming a major source of information on the Internet. After the technological barriers were conquered, agencies began to realize that Internet dissemination, or at least availability, was a wonderful model for disseminating information, for making routine information readily available, and for allowing consumers to conduct a variety of interactions with government without actually having to deal with an individual employee. The prospects for increased convenience, efficiency, and cost-savings seemed endless and, as a result, agencies provided a broad array of information, often without much forethought as to whether the information was essential. The mantra seemed to be to post as much information as possible and let users sort it out; whatever feedback the agency might get as to the usefulness of their Web sites could then be used to modify them accordingly, with the goal being to make the information as useful and convenient as possible.

This model abruptly changed in the aftermath of the terrorist attacks of September 11, 2001, as agencies began to rethink the availability of information. Because the Internet allowed universal access and made tracking individual users nearly impossible, agencies worried about how publicly available information might be used. It was clear that the terrorists had used public information sources in developing their plan. Suddenly, the idea that the more knowledge and information that was available the better was abandoned, and replaced with an essentially contrary conclusion, that information in the wrong hands could be used to hurt us. The immediate conclusion was that information should be restricted and, as a result, one of the consequences of 9/11 was to dismantle many public information resources.

The headlong rush to post information on the Internet during the 1990s was something of an anomaly as far as government information policy is concerned. Rather than being driven primarily by a political conclusion tied to the tradition of the right to know—that government is a repository of a vast wealth of information that it stockpiles and creates on behalf of the people and thus the people should have a presumptive right of access unless there are specific reasons for exempting certain types of information—the policy seems to have been driven more by a model derived from good business practices tied to the ideas of reinventing government and customer-friendly government services. The reinventing government policy, most closely identified with Vice President Al Gore, aimed to remake a bureaucracy that was typically seen as lethargic and inhospitable and to streamline it through the use of technology to make it more efficient and responsive to its customers. Information was an asset that allowed government to distinguish itself from the private sector. By making its huge repository of information more readily available, government provided resources and solutions that promised to make government more efficient.