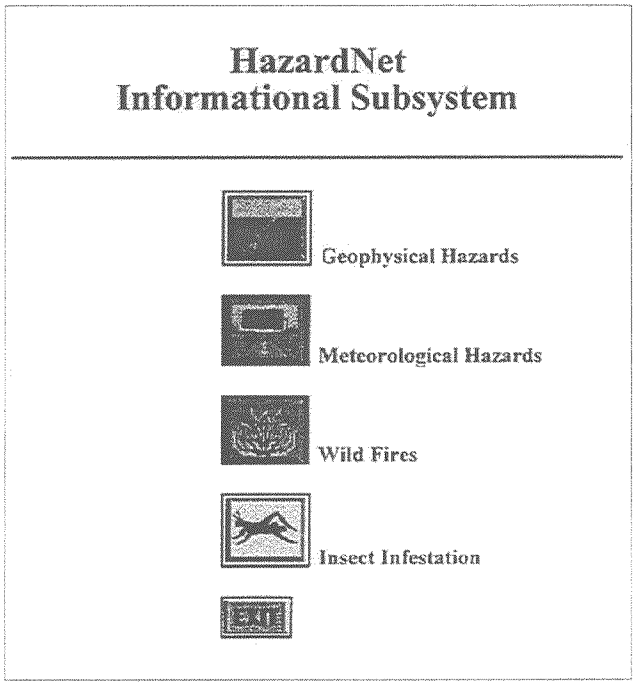
Informational Service—provides access to natural and technological information identified/categorized by hazard type. Each general category of hazard is identified by an icon. This is being done in an attempt to improve language independence and to accrete similar types of hazards under a common heading.

Operational Service—provides access to real-time hazard alerts, warnings and forecasts, situation reports, news accounts, Geographic Information System (GIS) along with country facts, demographics and other relevant information separated by hazard type. This service is to be used in monitoring early warnings and alerts in order to coordinate effective and timely international response.



Hazard/Disaster Situation Reporting—provides a mechanism for more timely, accurate and efficient collection and reporting of on-site information and for use in responding to an emergency.

IDNDR Home Page—provides access to the IDNDR Secretariat in Geneva, Switzerland and its wealth of hazard/disaster related resources. This service also points to other natural and technological hazard/disaster resources around the world.

Map of the World—presented to the user when entering HazardNet will be the basis for identifying locations of hazardous events. This map will be constantly updated to indicate countries where events are occurring. (Such events will be indicated either by creating a flashing display, by displaying the affected the country in a contrasting color, or by displaying an icon indicating the type of event.) By pointing and clicking to the location or icon the user will be able to acquire the latest status information related to the hazard/disaster as well as enter the GIS for use in

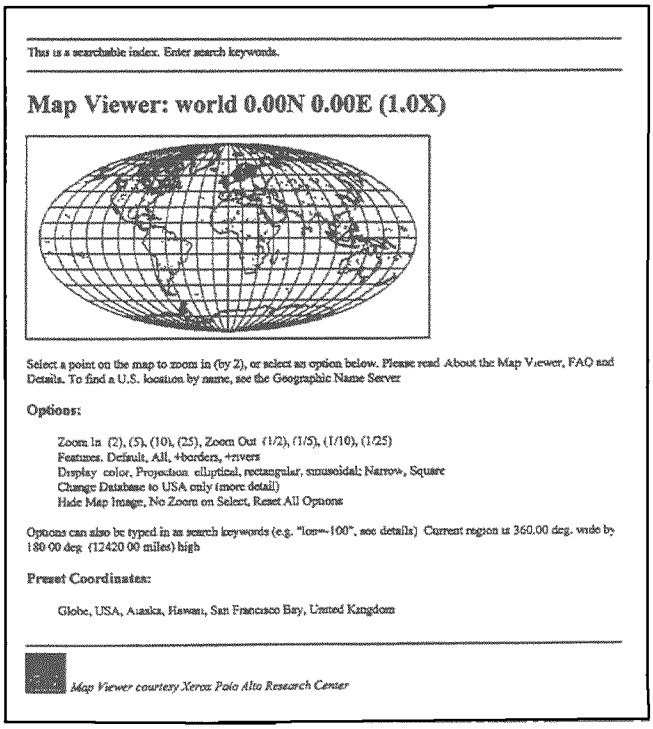
locating the disaster so that effective emergency management (including planning, response management and execution) can be accomplished.[48]

Although HazardNet is still under development, it already demonstrates the power of electronic information resources to integrate and facilitate the resources and activities of diverse disaster preparedness and response organizations.

4. Issues Posed by Information Technologies

a. Data Integrity

HazardNet and its predecessors, like the other examples of uses of information technologies—particularly the Internet— raise a number of significant issues, some of which are specifically related to the technologies involved. For example, electronic information has thus far proven difficult to authenticate and therefore often raises questions about provenance and integrity. These issues are presented in many different contexts. For example, one organization may provide accurate data, in an e-mail message or in a database, that is subsequently altered. The alteration may be deliberate (*e.g.*, by an agency or government wishing to exaggerate the extent of need or the quality of response being provided, or by an unauthorized user) or accidental (*e.g.*, a typographical error or mislabelling of data). In either case, subsequent users will be hard pressed to identify alterations because digital information is extraordinarily malleable: unlike printed or analog information, it is easily and undetectably altered.


This is a searchable index. Enter search keywords.

Map Viewer: world 0.00N 0.00E (1.0X)

Select a point on the map to zoom in (by 2), or select an option below. Please read About the Map Viewer, FAQ and Details. To find a U.S. location by name, see the Geographic Name Server

Options:

Zoom In (2), (5), (10), (25), Zoom Out (1/2), (1/5), (1/10), (1/25)
Features. Default, All, +borders, +rivers
Display color. Projection elliptical, rectangular, sinusoidal: Narrow, Square
Change Database to USA only (more detail)
Hide Map Image, No Zoom on Select, Reset All Options

Options can also be typed in as search keywords (e.g. "lon=-100", see details) Current region is 360.00 deg. wide by 180.00 deg. (12420.00 miles) high

Preset Coordinates:

Globe, USA, Alaska, Hawaii, San Francisco Bay, United Kingdom

Map Viewer courtesy Xerox Palo Alto Research Center

The quality of electronic information may also be at issue because it is often difficult to identify reliably the source of the data or the source may be unrecognizable. With most Internet services, it is easy to post data on an electronic server or bulletin board, without the "filters" of peer review or statistical analysis or the credibility of recognized institutions or publications. In fact, every Internet user is also a potential data supplier; consider, for example, the students at Kyoto

[48] *Id.*

City University of Foreign Studies whose reports about the Kyoto earthquake appeared alongside reports from the IFRCRCS and United Nations. The variety of lists of people killed by that earthquake raise similar issues: where are those lists from, how were they compiled, and who vouches for their accuracy? Even with the best of intentions, inaccurate, imprecise, or misidentified data may be posted to most Internet resources.

The accuracy of information provided on the Internet may also be compromised because of how that data is replicated and accessed. Many Internet databases, such as HazardNet, do not actually maintain all of the information they reference; instead, they provide electronic links to other data sets. This is a valuable attribute of these resources. But it also raises questions about what role the database provider, which may be clearly identified and highly reputable, plays in guaranteeing the authenticity and accuracy of data that the provider references but does not originate or control. This same powerful capacity of the Internet to support an unlimited number of links to the same data set also increases the likelihood that inaccurate or incomplete data will be made widely available or used for purposes for which it was never intended.

To date, Internet data providers deal with these issues by labeling their on-line resources as "experimental." Other, more lasting solutions are being tested, for example, providing electronic data "signatures" that could not be separated from a specific data file and that would indicate where that file was originated and whether it had been altered. Limiting access only to authorized users is another effective tool. However, any measure for guaranteeing data integrity that restricts access also limits the usefulness of the information resource and may increase its cost. In short, it has thus far proven difficult to guarantee the origin, authenticity, or accuracy of networked information without also compromising the very features that make networked information so valuable.

b. System Reliability and Capacity

To be valuable, information must not only be accurate, but also dependable. Thus far, electronic platforms, such as individual servers and the telephone or backbone links that connect them, have demonstrated uneven reliability. In the event of disaster or political or civil unrest, the technologies and the institutions that keep the Internet or other networks functioning are likely to be at risk. As many Internet users have found to their annoyance, heavy rains or high winds will often cause the network or some key component to "crash." Yet the experience following the Northridge and Kobe earthquakes suggest that these systems may be more reliable than first thought.

Even when complete failure is avoided, however, networks and servers face real limits in terms of speed and capacity. Some users following the Northridge and Kobe

earthquakes found important messages delayed or rejected because of high system usage; some servers were unavailable during periods of peak demand. Growing at a rate of approximately 141 percent per year, key transmission routes and services on the Internet already are overloaded and contributing to system "brown-outs." For example, commercial e-mail users in the United States, generating more than 44 million messages every month, are discovering that when electronic mailboxes are full (a function of technology and system operator preferences), excess e-mail is rejected, often without notification to either the sender or the recipient.

The key issue is not the current reliability of the Internet, but the need for certainty as to its future reliability. Dramatically escalating usage, increased privatization, and the fact that many key Internet links and resources are maintained by universities and companies with limited resources to guarantee system reliability, threaten the future stability of the Internet and warrant careful scrutiny.

c. Cost

Problems of accuracy, reliability, and capacity, while serious, are likely to be managed, if not solved, with technology. Other issues—such as how to pay the cost of these services and guarantee access to them—may not be dealt with so easily. Internet today is paid for through a combination of government and other public institutional support, connection charges, advertising, and direct subscriptions. There is little uniformity among users and among countries as to how much is paid or by whom. Under the current system, an outgrowth of Internet's origins as a government-funded network, few users pay the actual costs of their use and no users pay distance-sensitive costs. If one user in New York sends an e-mail to another user in Geneva, the sender may pay an access charge or subscription fee, but she is unlikely to pay her own "infrastructure" costs—they are most likely to be borne by an institutional intermediary, such as a university or employer—and she is certain not to pay the actual transmission cost (*e.g.*, the cost of a phone call from New York to Geneva). This may help explain the attractiveness to the users of the Internet as a communications medium.

As the Clinton Administration and other national governments move to privatize the Internet and eliminate government subsidies, more costs will almost certainly be passed onto users. An intercontinental e-mail message is unlikely to be free to the user, or billed only as a subscription fee or connection charge. Instead, like virtually all other telecommunications traffic, it will be billed at actual cost, based on the distance, data volume, or time involved. In the past year, commercial services have come to dominate the Internet. The move towards privatization and commercialization is accelerating, and with it will come increased pressure on information services to cover their costs. Most of the existing disaster-related databases rely on university and government

resources for their computing and storage capacity and Internet connections. These institutions are able to provide them, in part, because of their low cost. As those costs increase—and they are certain to do so—many government agencies and humanitarian and development assistance organizations are likely to feel the squeeze.

d. Access

Closely related to the issue of cost is that of access. As discussed above, access may be hindered by the disaster itself or by national regulations governing customs, broadcasting, and frequency assignments—what Hans Zimmerman described as the "sad experience of those who provide international humanitarian assistance in the age of information superhighways." These are not the only restrictions on access to information technologies. Important questions remained to be answered: Will disaster information services be available to all organizations, in more and less developed countries, who desire access? Will they be available in the field and in countries without data quality switched networks? Will they be available to organizations without network access or technological expertise? Will they, because of their power and flexibility, begin to replace information resources such as printed material? These questions, while important, are not intended to detract from the promise that information technologies hold for preventing and mitigating disasters. In many ways, precisely because of their versatility and lower cost, electronic information resources have the potential for dramatically expanding access. But the very real threat of escalating costs, regulatory obstacles, and the infrastructure and skill requirements to use these resources, should at least be the subject of full discussion.

e. Privacy, Intellectual Property, Liability, and Other Legal Issues

Information networks and databases must comply not only with the laws of the jurisdiction in which they are located, but also the laws of the jurisdiction in which they are received. For information resources available via Internet, that involves more than 100 separate national legal regimes, not to mention state or territorial laws. For example, in the United States, electronic image files containing photographs that were almost certainly not obscene in California, where they were located, were found to be obscene in Tennessee, where they were downloaded. As a result, the California operator was held liable under Tennessee law.

This is serious business for many national governments, concerned about the economic or cultural effects of unbridled information flows. As Anne Branscomb, author of *Who Owns Information?*, has written: "[t]he very existence of information

technology is threatening to nation states."[49] While obscenity laws are unlikely to be pose a problem for most disaster mitigation organizations, laws governing privacy and intellectual property may create greater risks.

Under the European Union's *Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data* ("Directive"),[50] all European countries will be required to enact laws protecting personal privacy and prohibiting the transmission of personal information to countries perceived as ignoring privacy concerns, for example, the United States.[51] Under the still-pending Directive, every EU member state would have to enact laws ensuring, among other things, that personal data—defined broadly by the Directive as "any information relating to an identified or identifiable natural person"[52]—must be accurate, relevant, not excessive and used only for the legitimate purposes for which it was collected. Personal data may be collected, processed, or transmitted only with the consent of the data subject. The collection and processing of data revealing "racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion . . . [or] concerning health or sexual life" is severely restricted.[53] The data subject must be informed and provided with certain mandatory disclosures if data is to be collected, processed and/or distributed to a third party, and he or she must have access to the data and the opportunity to object to its collection, processing and/or disclosure and to correct any factual errors.

How many relief workers could comply with these requirements in the field? How many organizations can guarantee that the information they post to the Internet meets these stringent requirements? Yet if the data is moved into or out of Europe, this is the law that will apply. Already, the British Data Protection Registrar, acting under national law, forbad a proposed sale of a British mailing list to a United States direct

---

[49] Anne W. Branscomb, "Global Governance of Global Networks A Survey of Transborder Data Flow in Transition," 36 *Vanderbilt Law Review* 985, 987 (1983).

[50] Com(92)422 Final SYN 287 (Oct 15, 1992).

[51] *Id.* art. 26 ("Member States shall provide that the transfer, whether temporary or permanent, to a third country of personal data which are undergoing processing or which have been collected with a view to processing may take place only if the third country in questions ensures an adequate level of protection").

[52] *Id.* art. 2(a).

[53] *Id.* art. 8.

mail organization.[54] The French *Commission nationale de l'informatique et des libertés* has required that identifying information be removed from patient records before they could be transferred to Belgium, Switzerland and the United States.[55] And Europe represents only one group of countries whose laws will be applicable to data on the Internet; there a diversity of other national regulatory structures in place for protecting personal privacy. Concern about privacy is growing around the world. Relief organizations are likely to face legal repercussions, as well as public and professional criticism, if the data they provide via the Internet violates the privacy norms of the many countries in which it is accessible.

Intellectual property laws pose similar concerns. In the United States, the Clinton Administration has interpreted existing copyright law to severely restrict copying, transmitting, or displaying electronic, copyrighted expression. Although copyright law protects only original expression, not facts or ideas, this interpretation would have the effect of protecting to electronic data itself, not just the manner in which it is expressed, by restricting access. That interpretation is widely ignored today and justifiably criticized. But if the Administration has its way, those restrictions will be clarified by Congress and the courts and be enforceable by any copyright owner whose work is infringed. In addition, as with privacy, information providers will have to contend with a wide variety of national copyright laws. Already, some data posted on the Internet is accompanied by instructions forbidding access by users in listed countries, in an effort to comply with those countries' laws that restrict access to such information.

Moreover, although the law is still unsettled in this area, some courts have extended liability related to electronic information to parties, other than the original provider, who help provide access to it. Disaster mitigation organizations, by providing electronic links to other databases and information services, may expose themselves to liability for the conduct of others who use those resources.

f. The Limits of Technology

Finally, we should be frank about the limits of technology. Information networks can convey words and images with great force and disseminate them more quickly, at lower cost, to a larger number of people than their printed counterparts, but these

---

[54] Office of the Data Protection Registrar, *Seventh Annual Report* 33-40 (London: Her Majesty's Stationers Office, 1990)

[55] Joel R. Reidenberg, "The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services," 60 *Fordham Law Review* S137, S163 (1992).

technologies seldom improve the quality, thoughtfulness, or precision of what is communicated. The power of information technologies includes the power to mesmerize, to distract, to substitute form for content. Against that very real possibility, we should always be on our guard.

CONCLUSION

Communications technologies and other resources are essential, cost-effective tools of disaster mitigation. They are indispensable to predict, track, and provide early warning of natural hazards; link relief officials with governments, affected populations, and sources of emergency relief supplies; improve intra- and inter-organizational management and cooperation; facilitate rational deliberation by scientists, engineers, government officials, other disaster response officials, insurers, the media, and the public; and educate the public about natural hazards and disaster prevention. Increasingly, disaster preparedness and response organizations, both public and private, have come to recognize the vital link between effective communications and disaster mitigation. Yet each of these uses also raises important issues that the disaster community has been slower to respond to and act on. Perhaps the most important and least addressed are those issues raised by the use of information technologies by disaster mitigation organizations to communicate with each other and the public and to share information resources through networks. The potential of the technologies involved should only expand our interest in examining and addressing those issues, particularly concerns about cost and access. The failure to do so will certainly threaten our capacity today and in the future to employ the power of communications to avert disasters and to save lives.

About the Author

Fred H. Cate is an Associate Professor of Law and Faculty Advisor to the *Federal Communications Law Journal* at the Indiana University School of Law-Bloomington, and a Senior Fellow of The Annenberg Washington Program in Communications Policy Studies.

He was a delegate to the 1991 Conference on Disaster Communications in Tampere,Finland; co-convener of the 1993 Roundtable on Media, Disaster Relief, and Images of the Developing World in Washington and London; and convener of the 1994 Roundtable on The Media, Scientific Information and Disasters at the United Nations World Conference on Natural Disaster Reduction in Yokohama, Japan. He is the editor of *International Disaster Communications: Harnessing the Power of Communications to Avert Disasters and SaveLives* (Washington, D.C.: The Annenberg Washington Program, 1994), and the author of *Media, Disaster Relief and Images of the Developing World* (Washington, D.C.: The Annenberg Washington Program, 1994), and "Communications, Policy Making, and Humanitarian Crises," forthcoming in *Humanitarian Crises, Policy Making, and the Media: Strengthening Interaction in the Electronic Age.*

Professor Cate can be reached at the Indiana University School of Law-Bloomington, Bloomington, Indiana 47405, telephone (812) 855-1161, facsimile (812) 855-2259/0555, Internet fcate@indiana.edu

The author gratefully acknowledges the thoughtful assistance of Edward Gross of the U.S. National Oceanographic and Atmospheric Administration.