

E-GOVERNMENT: IS E-DEMOCRACY INEVITABLE?*

AUTHORS: **Craig J. Blakeley**
 (CBlakeley@AllianceLawGroup.com)
 Jeffrey H. Matsuura
 (JMatsuura@AllianceLawGroup.com)

Alliance Law Group LLC
8614 Westwood Center Drive, Suite 450
Tysons Corner, VA 22182
USA

Abstract **E-government often is thought to lead, almost invariably, to e-democracy, by improving governmental transparency, expanding the information flow between governments and citizens, and enabling citizens to exercise more effective control of governmental institutions. We believe that such results, while desirable, are not inevitable. Instead, we believe that e-government is a more neutral factor that can be used to support non-democratic regimes and values as well. E-government development and implementation, both domestically and internationally, should be undertaken with an awareness of this risk.**

E-government is typically perceived as a positive development, helping to make governments more efficient internally, through improved communication, reduction of duplication, and transaction automation. E-government is thought to increase transparency of governmental functions, both to businesses and citizens, and to result in a more “customer-oriented,” responsive, approach by government. Through e-government, citizens and businesses are believed to gain ready access to governmental information and operations. The end result of this process is often thought to be a major restructuring of power between government and its citizens, enabling citizens more effectively to control government and guide its functions (perhaps even on a day-to-day basis) through electronic voting and other types of electronically interactive participation made possible by the Internet.

We believe, however, that such developments, while welcome, are not inevitable. Rather, we believe that the potential risks of e-government must also be

* Prepared for “*Innovations for an e-Society. Challenges for Technology Assessment.*” (Berlin, Germany; Oct 17 – 19, 2001).

recognized and addressed. Like the Internet, e-government is neither good nor bad in itself but can be used or misused to achieve and further the goals of the particular society in which it operates, or to obstruct pursuit of those goals. A democratic and open society may use e-government to become even more open and democratic. Conversely, a closed, tightly controlled society, may use e-government to assert even more control over the day-to-day lives of its citizens. Existing democratic countries also may implement e-government initiatives in ways that offer the potential to undermine, rather than reinforce, important societal and political values. Thus, whether e-government initiatives will result in movement toward e-democracy depends upon the social and political environment in which they are implemented and the effectiveness of those implementation efforts.

If e-government is to be used to advance e-democracy, we believe that it needs to be viewed in a more realistic manner – in much the same way that our understanding of e-commerce has developed. Who can forget those early days of e-commerce and the “dot com” phenomenon, when traditional business rules were thought to be a thing of the past – when any company could simply put “.com” behind its name and become an overnight success (without worrying about such mundane issues as profitability and the bottom line)? That early, and unrealistic, perspective now has been abandoned. Instead, it has been recognized e-commerce is not an answer in itself but a tool to be used, or misused; strong companies will use the Internet and e-commerce to become stronger and weak companies, Internet or not, will fail. So, too, it is with e-government.

To contribute to a more balanced and (we believe) realistic perspective on e-government, this paper provides a discussion of e-government in the context of non-democratic governments. For purposes of that discussion, we have chosen three areas that we believe are among those commonly regarded as central to e-government: Internet access; information flow; and efficiency. Each of these is discussed below.

Internet Access

E-government requires online access for its success – for communication between governmental agencies and departments and between the government and the outside world. Internet access often is thought to result in increased democratization,

as citizens are provided with access to additional sources of information, uncontrolled by the government and as they gain access to e-mail with which they can receive and send messages uncensored by the government. However, these conclusions are based on a number of assumptions that we believe are unwarranted, at least in the context of authoritarian governments.

First, there is no reason to believe that Internet access will be provided in a manner that is free from government oversight, review, or even active government interception. These goals can be accomplished in a number of ways.

One way is through government ownership of the Internet service or access provider. In Syria, for example, domestic Internet access is a relatively new phenomenon, inaugurated under President Bashar Al-Assad. However, Internet access is available only through a government-owned provider, thus furnishing the opportunity for government-imposed limitations on the sites that may be accessed. In addition, this provides the opportunity for government review and censorship of private e-mail. In that regard, the authors have been advised that it sometimes takes 24 hours or more for e-mail sent to or from a Syrian address to reach its intended recipient; presumably the delay is caused by review of the e-mail by Syrian government censors. Moreover, according to sources believed by the authors to be reliable, an individual who redistributed via e-mail a politically sensitive message within Syria has been imprisoned by Syrian authorities. As a consequence of such actions, the authors have been advised to transmit potentially sensitive or confidential information to Syria via fax, which presumably is less susceptible to government interception and monitoring, rather than by e-mail.

Government ownership of the Internet access provider is not the only way in which the government may monitor or control Internet usage by its citizens. The government may make it illegal to access certain Web sites or sites containing certain types of content and may impose on private Internet access providers the legal obligation to monitor or restrict such access. For example, in China, the government requires Internet companies, including Internet cafes, to be licensed and to furnish to the government upon request, lists of those individuals who have connected to their facilities or servers. In a recent article in the Washington Post, it has also been

suggested that America Online would comply with Chinese government request to furnish it with names of subscribers, and other identifying information. *“You’ve Got Dissidents? AOL Weighs China Market – and Rights Issues,”* Washington Post, p. A1 (August 29, 2001).

Even as governments move to enable e-government functions, they may act to restrict the ability of their citizens to access the Internet. In Cuba, for example, the central government has taken a number of e-government initiatives, including Infomed, a medical information network operated by the Cuban Ministry of Public Health. This connects medical centers around the country and provides online access to electronic journals and searchable databases. It also provides an international e-mail link. Some government publications also are available online, including *Granma*. A number of state-owned tourist agencies also have online sites designed to attract foreign tourists and capital to Cuba.

Notwithstanding such efforts, Internet access in Cuba is carefully controlled. Internet access is almost never permitted from home and is limited to a few universities and other government institutions. Of the estimated 110,000 computers in Cuba, approximately 2,000 have full access to the World Wide Web. Future plans call for expanding the existing Cubaweb (a Cuba intranet) and permitting access to it and national (but not international) e-mail through computing clubs and post offices. (See Kalathil & Boas, *The Internet and State Control in Authoritarian Regimes: China, Cuba and the Counterrevolution*. Carnegie Endowment for International Peace, (July, 2001) for a detailed analysis and comparison of the efforts of China and Cuba to control and manage Internet development) (<http://www.ceip.org/files/pdf/21KalathilBoas.pdf>).

Improved Flow of Information

One of the operative assumptions of proponents of e-government is that e-government initiatives will lead to improved information flow both inside and outside of government and that this, in turn, will lead to a democratization (or e-democratization) of society. While we agree that e-government is likely to improve the flow of information, we question whether this will necessarily foster a trend toward democracy. To the contrary, we are concerned that the improved information

collection and distribution mechanism afforded by e-government may be used by authoritarian regimes to more effectively assert their control over the populace, to distribute misinformation or propaganda to both domestic and international audiences, and to gather information about their citizenry.

For example, China is engaged in the “informatization” of government – a process designed to strengthen state processes and centralize control in Beijing by transforming the bureaucracy through e-government. In so doing, “the regime seeks to streamline many of its government operations through networked information management and to consolidate Beijing’s central authority through more efficient communication with provincial governments.” (*Kalathil & Boas*, pp. 8-9).

A number of countries and areas, including China, Cuba, Saudi Arabia, Palestine, and others, also actively use the Internet to distribute their own viewpoint or propaganda, both internally and externally. Governments may also use the Internet to distribute “disinformation” -- for example, by setting up Internet sites that appear to be operated by bona fide dissident groups but which are actually operated by government agents for the purpose of discrediting the real dissident organization or identifying its supporters. In a benign example of such a technique in the United States, the Federal Trade Commission has arranged with various search engines to list FTC created “get rich quick” Web sites in response to searches for such sites. When the user accesses the site, he or she sees, not the expected site, but an FTC warning about the dangers of such sites, including consumer fraud. On a more straightforward level, both China and Cuba are reportedly in the process of setting up their own national intranets where, presumably, content will be carefully controlled and sanitized for domestic consumption.

The Internet offers governments an enhanced capability to collect and analyze data concerning its citizens. The collection and potential misuse of private information collected from consumers by online companies is well-documented as is the use of cookies and other types of tracking devices in private e-commerce transactions. The U.S. government has been criticized for failing to adhere to its own announced privacy policies on its e-government sites. One of the notable failures in

that regard was the initial use of cookies on the portal to U.S. government Web sites – www.egov.gov – contrary to the stated privacy policy on that site.

Governments already have access to a broad range of sensitive information concerning individual income, health and other information. The Internet offers the ability to expand this already extensive data collection network and to share and analyze it both domestically and internationally. There is no reason to believe that an authoritarian government would not attempt to take full advantage of this enhanced capability provided by the Internet.

Even democratically elected governments, such as the United Kingdom, may find themselves tempted by this capability. There, the government has adopted the Regulation of Investigatory Powers Act 2000. (<http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm>). That law, among other things, gives the government the right to demand the key or password to any data there is some lawful authority to obtain and prohibits the individual from whom the key is obtained from divulging to third parties the fact that they key has been disclosed.

Improvement in Governmental Efficiency

It is widely predicted that e-government initiatives will dramatically increase governmental efficiency, by improving internal government communication, reducing duplication and inefficiency, and ultimately resulting in a more “customer-oriented” government. We do not disagree with this conclusion. But even if it proves to be accurate, we do not believe that such improvements in governmental efficiency and functioning (however dramatic) **necessarily** will foster a trend toward e-democracy.

Efficiency is a value-neutral proposition that can be applied equally well to a democratic or authoritarian government. It simply enables governments to do better and at less cost than which they already are doing. We have already discussed the possible use of the Internet and e-government to enable more effective monitoring of citizen activity.

In addition, the effective use of e-government may reduce domestic pressures for political change. For example, one of the recognized purposes and desired effects of e-government is to increase the transparency of governmental functions and, thereby reduce the opportunity for corruption. Corruption (and the enrichment of government officials that accompanies it) is a well-recognized source of citizen frustration and disenchantment and, as a consequence, a potential source of citizen unrest and political change. By helping reduce corruption, e-government initiatives may help preserve incumbent authoritarian governments.

In China, for example, the State Council and Ministry of Information Industry have begun online auctions, in part to reduce corruption in the award of government contracts and to increase transparency. In so doing, the government apparently hopes that the threat posed by corruption to the government's authority and to its modernization plans will be reduced.

CONCLUSION

It was once thought that the "Internet economy" had replaced the traditional economy – particularly in the United States – and that the peaks and valleys of the traditional business cycle were a thing of the past. The present economic downturn in the U.S. strongly suggests that the transformative effect of the Internet upon the private economy has been substantially overstated. We believe that the same is true with respect to e-government.

E-government does not appear to us to be an independent force for governmental openness and citizen participation that will lead inevitably to e-democracy. Rather, we believe it to be a far more neutral factor that will derive its value proposition from the context of the society and government in which it is applied. If implemented with proper legal and technological safeguards, it will enhance and support democratic principles in existing democracies. These standards should encompass, among other things, legal protections for individual privacy, including standards for the collection and sharing of data by and between governments and between governments and private companies or organizations.

It is also important to remember that governments may change over time. Today's benign, progressive government can evolve into tomorrow's despotic regime, yet the infrastructure of e-government will live on and will be available for use by both benevolent and tyrannical leaders alike.

With respect to non-democratic governments, it is possible that e-government may result in liberalization or democratization of such governments. However, particularly in the short or middle term, it is likely that such governments will seek to utilize e-government initiatives to extend the control they currently exercise over their citizens and to perpetuate presently authoritarian regimes.

We remain hopeful that, in the long run, e-government will support the development of e-democracy. However, in order for this to occur, we submit that it must be approached less as an article of faith (in which e-government is believed to **necessarily** lead to e-democracy) and more as a goal which is striven for in a thoughtful, disciplined manner. Only by recognizing and addressing the possible risks of e-government, may its potential benefits be fully realized.