What We Owe the Citizen
Peter Alterman

In recent months we have all seen dramatic changes in the way the Federal government approaches electronic media. Coupled to President Obama's Openness and Transparency mandates are the visible role web-based social media outreach contributed to his November victory and his call for technology to play a key role in reshaping the way government does business, particularly bringing citizens into government decisionmaking.

Many inside and outside government, therefore, are touting the transformational aspects of new technology adoption. It's easy to get carried away with this kind of rhetoric, and this is where greybeards (such as myself) have the advantage of the long view, because what's new, what's transformational, depends on your perspective. To the Millennial, new media really is transformational, that is, it changes the way one interacts with the world. YouTube, FaceBook, MySpace, Second Life, Hulu, Twitter, widgets and gadgets and such are all wonderful tools for engaging in a social world devoid of physical contact. It is no stretch of the imagination at all to see why younger folk (and older folk who would be *au courant*) would be eager to embrace them. The connection between these virtual social environments and the previous generation of role-playing video games on Xbox, Wii and PlayStation that the Millenials grew up playing is easy to trace.

To me, who entered government when the cutting edge of technology was the IBM Correcting Selectric typewriter, "transformational" has another meaning altogether. For me, the transformational technology has been the PC, because the result of that change was the all but total disappearance of the professional secretary from all but the most senior government offices, where she or he is more of a status symbol than a necessity. When every professional had a PC with a word processor, no secretary was needed to do all the typing, because correcting typing errors had become painless. And then, of course, there was e-mail, which obviated the need for memos to be typed in the first place. And on and on. If you think the disappearance of a whole class of office worker in under five years – more or less from about 1985 to 1990 - wasn't transformational, your definition needs refinement.

And yet the real transformation in the government workplace actually started with the invention of the computing machine during World War II. The first time an ENIAC turned from calculating radar vectors to sorting census cards the rush to office automation had begun. By the time I entered the government, mainframe computers were everywhere, processing large batch jobs. Input devices were limited to card punches and card readers; output devices were limited to line printers and other impact devices, but the seeds of the desktop computer was already there.

With the benefit of hindsight, we now can see that the first two rounds of technology transformation in the workplace were mostly about replacing humans with machines. Within government, in fact, replacing bodies with machines was explicit and was required justification for approval to purchase computer systems, software and services.

Procurement of automatic data processing stuff was acceptable on the basis of lowering program costs, or said another way, as a basis for raising productivity. While the first goal was rarely, if ever, met, the second surely was.

Behind this significant approach there was also another thing happening: the new computing machines, now linked together by coaxial cables into networks, offered the possibility to acquire, store and manipulate information in unexpected and new ways. I still remember the shock I felt when I first encountered a hyperlink in a document. I could read along, stop and click on a hyperlink in the text, and be taken to *another* document, or a picture, or eventually a website. A linear process had become multidimensional on an unimaginable scale. Unfortunately, there was – and continues to be – no generally-accepted way to measure the value of this new capability – information integration in *n* dimensions - in the workplace.

So we can see that everything that's happened so far - the mainframe, the PC, the network, the Internet, Web 2.0 - all this has been part of an ongoing transformation that is far from being played out. What society will look like at some random point down the timeline is anybody's guess, no matter what the bloggers or the professional futurists claim. What I'm saying is that transformation is a process, one that I suspect we are nowhere near exhausting.

And yet, in the process of adapting to this technological revolution over the past 60+ years,  the government has recognized and adopted (sometimes inadvertently) fundamental principles which I call What We Owe The Citizen. We can think of these as the general categories of value that Information Technology offers to the consumer of government services. Think of this as a way of capturing the value of information technology at the end of the spigot. Summarized, we owe citizens:

1. Trustworthy Information,
2. Information they want, when they want it,
3. User-friendly interfaces, and
4. Protection of their privacy.

We have laws, policies and practices designed to give the citizen these services.

Trustworthy information means that the citizen knows the information she gets from a government website actually comes from a government website, not a fraudulent one masquerading as a government site. The information is deemed accurate before posting or the degree of its authoritativeness is openly acknowledged. The citizen gets the information she seeks, not a hacked or fraudulent version.

In order to provide these basics, government networks must be secure, sites must be managed and monitored, online applications be production-hardened and data protected. These requirements drive the need for effective cybersecurity and for active, conscientious management of information  posted on government sites, for non-commercial bias and, to the extent possible, for non-political bias. More and more lately,

trustworthiness includes knowing who is accessing government sites at particular levels of assurance of identity comparable to the risk of harm or damage to the site by fraud, hacking, etc. Identity management and identity federations are key to this last element.

Providing information citizens want speaks directly to President Obama's Transparency and Openness Initiative. Citizens want to know what information the government has, what information it uses to make policy and statutory decisions, how decisions are made and why, and where the money is going. In a participatory democracy such as ours, these wants are rights, since politicians govern and federal employees work on behalf of the citizens.

Being able to provide information citizens want requires the government to report on its activities and make those reports available. It also implies that the citizen must be able to tell the government what information he wants to see, and therefore feedback and communication with citizens is part of delivering on this principle. Government provides for outreach and input, often required in statute, in many ways. Online methods for interaction are signature features of the current crop of new online applications (media), but the purpose of implementing them is not new. Thinking that new media are enabling new behaviors is an error born of lack of perspective.

User-friendly interfaces to online information are where many of the real technology innovations occur. As I've mentioned, in the Good Old Days, one interacted with a computer through punch cards and line printers. The appearance of the 9-inch amber dot-matrix screen and keyboard for computer interface was revolutionary (I know, I was there). The change from DOS and UNIX command lines to the graphical user interface, with mouse, was revolutionary (I know, I was there). The first browser on a www site was revolutionary. Note that we're still working on a simple, reliable voice interface.

The point of user interfaces, after all, is to make the citizen's ability to find and access information she wants as simple as possible. This goal points at the ergonomics of web design, a field that has matured over the past twenty years, but it also points at the citizen (voting, tax-paying citizen) who is blind, or deaf, or paralyzed. Government has an obligation that commercial or private sites do not have: the obligation to serve all its citizens. Hence, Section 508, a law, mandates that government websites and applications in general be designed in such a way as to be accessible to citizens with a wide variety of disabilities.

Since service to the citizen is the underlying principle of the government, providing user-friendly interfaces to government information to all citizens is clearly more important than enabling the latest technology gadgets or widgets – generically interfaces - no matter how clever or trendy they may be considered. We must remember that technology is always in service to the program, not vice versa. One may argue that this principle requires the government to accessibility-enable the ever-latest round of new interfaces, and I would tend to agree with that view as a general proposition. Nevertheless, it's likely that there will usually be a gap, significant or otherwise, between the new interface and the accessible version of the new interface, and in those cases, service to the citizen

should always be the goal of implementing the latest technology.

Finally, protecting the privacy of Personally Identifiable Information (PII) in IT systems and during digital transactions has been a high priority for Federal systems since the Seventies, and with identity theft rampant these days, this priority is only increasing. Government has historically dealt with this requirement in two ways: first, by limiting and minimizing the amount and kinds of PII systems capture and save and then by securing the systems that store received PII.  As we know, sometimes this requirement has been honored more in the breach than in practice.

The fact that many (some would say most) commercial systems do not protect PII with anything near the rigor of government systems does not mean that we should migrate in that direction; rather, their systems should emulate and adopt our privacy protection policies.  It goes without saying that we should live up to our responsibilities, as well. Again, the goal is to provide what the citizen deserves and privacy protection is always more important than ease of implementation or trendy interfaces.

These four principles have emerged from our experience implementing successive waves of advanced information technologies.  They are our guideposts moving forward as we adopt and adapt to ever more advanced capabilities.  Our citizens deserve nothing less.