New Challenges For democracy

Better access to information yield also efficient propapanda

One would think that better access to information would improve the knowledge of the masses and therefore the democratic values would be reinforced. But that's without taking into account that access to information doesn't mean necessarily access to good, valuable, information, it can also mean access to fake, made up, rumor-based, conspiratory information used for propaganda sake. It is easier to make people believe what a small group wants, because of the ease of spreading out information. Terrorist groups recruit using online technology.

International relations

Countries are able to limit access to information available globally on the Internet. The Great Chinese Wall for example is now an Internet wall.1

Modernization

The picture is contrasted. On the one hand, better access to information for more people means that an increasing number of us are able to access to the sources of knowledge that are used to make decisions, and therefore the overall democratic coverage is increasing. USSR failed because it was eventually not able to prevent communication using new technologies, such as fax messages in the 1980s2. USA

may fail because it is not able to contain damages made to its information by foreign countries, including Russia.

Computers, cell phones, digital cameras, have become ubiquitous. Citizens use their ability to film and transmit images and text at the speed of light to improve news coverage over the world. Online discussions, blogs, wikis, and many of such technologies help bring people together to discuss issues that concern them. These phenonema occur worldwide, and help bringing people together and make the world smaller. It is the same technologies that enable work to be performed overseas. The rise of Asia, from India to China, has much to do with the availability of information technologies.

At the same time as the world economy becomes global, other phenomena become global, and the desire for world domination based on one single school of thought, Islamic fundamentalism, seems to be the common ground for those who have adopted terrorism as one of their means. In other words, terrorists are more than just terrorists. They have goals they want to achieve, and they are motivated enough for some of their adepts to accept to kill themselves in suicide bombing operations. Terrorists are also propagandists, they benefit from anyweakness shown by Western democracies, including the lack of attractiveness and the seemingly impossibility to solve internal ongoing inequalities and other societal problems. Terrorist organizations use the same technologies as everybody else to achieve their goals. The ability to browse information online is useful therefore not only to extend the span of democratic powers, but also to those forces which want to destroy democracy. The need for protecting information, the efficiency of what is called "firewalls", is therefore essential.

At the same time, the ability for citizens to access information which may prove to be crucial for them is also essential. The challenge is to find the limits between what can be displayed and what can be considered a public threat. For example, preparedness to disasters is essential to ensure that citizens will know how to cope if they are confronted with an actual disaster. But by displaying disaster scenarios, is also showing where the Achille heels of a society are. In order to be able to do this, it is necessary to understand how information is flowing in a very detailed way. For example, when leaks occur, it is therefore important to be able to investigate

inside the information system to understand how it could have happened and prevent another one to happen again. In order to be able to accomplish that, a deep knowledge of the processes contained in an information system is needed.

Voting machines

Contrarily to commonly held belief, using technology not only doesn't solve all problems, but sometimes, it creates new ones. Because of numerous problems that have been reported, voting machines have been removed in various states, for lack of accountability: There was no way to establish whether any reliable results could be established by using them.[footnote: The web site [http://www.votingmachinesprocon.org ||http://www.votingmachinesprocon.org] compares opinions for and against using voting machines.] Denise Lamb, former Director of Elections for the State of New Mexico, describes the auditing process, and mentions, interestingly enough, that auditing is performed by certified public accountants. Darryl R. Wold, former chairman of the Federal Election Commission, explains that paper records simply consisting of ballots printed by the computer after the closing of the polls are never seen by the voters and cannot reliably indicate that the data stored in the computer are accurate.[footnote: See [http://www.votingmachinesprocon.org/questions/audit.htm||http://www.votingmachinesprocon.org/questions/audit.htm]] To this I can add that if the voter would be requested to vote twice, once electronically, and once with a paper vote, then there would be no way to eliminate errors coming from the fact that voters may have casted two different votes, electronically and on paper. Therefore, any discrepancy between paper records and electronic votes stored could not be attributed for sure to a software error. Unless it would be possible to look inside the process used by the software and hardware as it would be a transparent glass box, auditing of the voting machines will remain a difficult task. The only way out seems to be a constant monitoring of everything that happens within the software that is used to record the votes, and conduct extensive tests by different parties, including - and especially by - those which are not members of the company producing the software. Therefore the software used for recording votes mustbe modular,

extremely clear to read, and of course the source code should be made public so as to allow a community of hackers and citizens to examine the software in all its components and so opening the possibility of detecting any flaw. As long as the software for vendor machines remains proprietary and is only accessible to the company that produces it, democracy is in serious jeopardy. The only way forward seems to be not enable use of voting machines unless the process is open enough to be considered reliable. Public interest groups almost universally supported the move to optical scanning, which is now thought more reliable than touch-screen voting, if only because it leaves a paper trail.[footnote: Abby Goodnough, "Vote Giving Florida New Headache", New York Times, October 13, 2007.]

Border Security

Heavy reliance on technology for border security helps, but it does not replace adequate training of the personnel responsible for ensuring security. Connecting information about individuals so that every immigration officer in the airports can immediately see whether an individual is mentioned in a list of suspected persons maybe a good thing, but it is not error-prone. Some people have got into trouble because their name is identical or similar to the name of a person who is on the list of suspected individuals. The limitations of the technologies used to find information need to be further investigated, to ensure that the proper information is returned when needed.

It is likely, although no information is for obvious reasons publicly available to prove it, that use of high technology equipment has helped to detect terrorists trying to cross borders. But this can not be the only solution. Israeli security, which is considered to be one of the best in the world, perhaps the best, relies on other factors than simply technological. It relies in the ability for the security personnel to detect suspect behavior by asking questions that may lead to contradictions, or distabilization, and may indicate that the person being questioned may be hiding some crucial information.

E-Government

Governments encourage the use of technologies to improve their relations with their citizens. In the United States, the e-Government initiative has been in place since the early 2000s and it is now possible to find practically all materials issued by the government, such as forms, and related instructions, and download directly from any computers. In other parts of the world, Europe and Asia namely, similar initiatives exist, and have contributed to ease the relation of national, or regional administrations with their citizens. It is obviously more convenient, because for example, to get a specific form, it is not necessary to order by mail or to ask for a leave in order to wait in line for hours, during business days, just to be able to get a given form. The Federal Enterprise Architecture (FEA) was initiated on February 6, 2002. Its purpose is to provide a "more citizen-centered, customer-focused government that maximizes technology investment to better achievemission outcomes." [footnote: [http://www.whitehouse.gov/omb/egov/a-1-fea.html||http://www.whitehouse.gov/omb/egov/a-1-fea.html] .] What this concretely means is that you can't find an office within the governement (and elsewhere) without computers in it. All information is now processed electronically. The ability to file tax returns on line is an improvement, but it also means that the governments have more information easily available on each of us than they ever had before. Some information gathering that was hard to get has been greatly facilitated. From the point of the view of the government, this may be a great thing. But from the point of view of each citizen, things are not so rosy. This means that there is a potential that didn't exist before for mis-using the information now available, and privacy has decreased. Whether we want it or not, we have less information which is strictly private. This is not only by accessing information through an actual computer. We all know that all the operations we do with credit or debit cards, and all our phone conversations, especially with cell phones, are recorded and are used to feed huge databases, that are – or were – intended to be used mainly for statistical analysis. But still, there is a potential for misuse this information and this temptation is very easy to grab for a government that for some reason decides that it is in the highest interest of the country to exploit this information. Eavesdropping has now become a

component of the society that has become so widespread that nobody seems to complain any more, or to have any hope to be able to go against it. For enterprise-wide policies, prominent industry standards have been adopted, such as XML and Web-related technologies. The adoption of technology-based solutions have also had the effect to increase the power of technologists, who decide of the architecture of the systems. It sometimes results into a loss of accountability: How many times do we hear that the source of a problem is the computer system, on which the employees we talk with decline any responsability. The governments are like any other consumer of technological products, they purchase what is available on the market. But the limitations of the products often determine the boundaries of what can be done. And then it becomes a matter of consensus that there are things that simply cannot be done because no product exists that is able to implement them. The relationship between users and vendors is of crucial importance. Several powerful companies and organizations, and the government is among those, are able to make vendors create new products adjusted to their specific needs if they do not find any product currently available that satisfies their needs. It is interesting to note however that the government technology czars do not often take advantage of their power, and instead behave as regular users of several products made by big software corporations. It is time to switch to a user-centric technology-driven society rather than to stay stuck with a technologist-driven/impotent users schema which is still dominant today. The reason this happens is mainly due to an exaggerated trust in experts who are supposed to know what is right and what is wrong and are able to do so without encurring any contradiction, because they are experts. This magical power is of the same nature than the one from physicians who are considered to "know better" when they sometimes are guessing and improvising more often than the patient really wants to know. We are aware that medical errors do occur, but we prefer to think that it only happens to others. But also to the inabilityto think about the problem to solve in terms that can be understood by those who are directly related to it. There are many hidden complexities and subtleties in the technology that people don't want to hear about. They prefer to delegate part of their power to those in charge of handling the tools. This works fine, provided we don't look too closely at the results obtained versus the amounts of money spent. We also have to recognize the role of innovation and experimentation: therefore when a project doesn't come into full fruition, it's not necessary a bad thing, it may

be because it was not mature. Leaving room for experimentation is good. But there are cases where the context is clearly not experimentation, and results are not achieved as expected.

Healthcare

The digital mess appears in all its crudeness in the healthcare industry. The part of medical information which is digitized is still small. Increasing its scale would have big advantages, providing more reliable, centralized, information about the medical history of each of us. Even if we forget to tell our physician that we are taking such a pill, this information will be recorded. However, the difficulties abound. Nothing is more private than personal medical information. There are good reasons for not wanting to share such information, including with our closed friends and relatives. Even less so with employers and insurance companies, who we may not want to tell about our medical problems. There is a fundamental right to privacy, which is in principle protected by the Fourth Amendment of the US constitution. If the physicians record the medicines they prescribe to us, it doesn't necessarily mean that we have taken them. There is a chance that we would be regarded as having taken that drug, but really all what is possible to know is that this drug had been prescribed. We may even have bought them, but still not taking them. This situation may be extreme, or juged absurb – what is the point of throwing money out through the window? – but it can happen, and sure enough, it actually happened more than once.

Unified way of thinking

Information technologies create new threats to democracy. The temptation exists to reduce information to what computers are able to handle. Since computers need data to be unambiguous to be useful, data are encoded following models which have been elaborated usually with the computer in mind, which may sometimes

result in oversimplification and in imposing views that are reducing complex realities to a set of well-defined, but over- simplified items. This problem can prevent free expression of complex and messy information. It usually prevents also conflicting information to be entered into a computer system. This results in a situation where the information encoded may not reflect the reality, or worse, may prevent personnel to enter data according to perspectives which are different from those which were originally allowed by the designers of the system. The gravity of this problem can be minimized by saying: we have been through this already. For example when desktop publishing systems replaced typesetting systems, professionals in the typesetting industry were complaining about the limitations of the computer-based systems and the loss of functionalities that followed. But this was a temporary problem, due to the nascent industry. Loss of content is much more serious, because it can't be recovered. We need to do something about it. The second part of this book presents solutions toavoid having to reduce information to whatever current computer software applications are able to absorb.

The Problem With Taxonomies and Ontologies:

Ontology, Schmontology, Entelechy

• Ontology: What things ought to be • Schmontology: The painful discovery that they are not behaving as expected, and • Entelechy: what they end up to be.

Taxonomy: classification challenges

Philosophically speaking, an ontology is a science or study of being: “specifically, a branch of metaphysics relating to the nature and relations of being; a particular

system according to which problems of the nature of being are investigated; first philosophy". [footnote: Dnyanesh Rajpathak, Knowledge Media Institute, The Open University, d.g.rajpathak@open.ac.uk, [http://kmi.open.ac.uk/people/dnyanesh/Publications/ontology-1.ppt||http://kmi.open.ac.uk/people/dnyanesh/Publications/ontology-1.ppt]] In computer science, "an ontology is the attempt to formulate an exhaustive and rigorous conceptual schema within a given domain, typically a hierarchical data structure containing all the relevant entities and their relationships and rules (theorems, regulations) within that domain."[footnote: This definition of "ontology" was found in [http://www.wikipedia.org||Wikipedia] . As Wikipedia is being edited, the definition has changed, and this quotation is not there any more. The side-effect of the web-based publication process is that there is no way to guarantee stability of information and especially of sources. However, in this case, this definition has been quoted by several authors who all refer to the Wikipedia origin that doesn't exist any more.] Using the philosophical term in the computer science context has a misleading effect: it conveys the idea that it is in the nature of things that they are the way we describe them. However, although things do exist, they cannot be described without a specific world viewworld view, be it implicit or explicit. Therefore there are various ways to describe the same thing, each of which is valid in its own right. Variations may be due (among other reasons) either to the fact that the descriptions have been created by different unrelated authors, or that they apply to different contexts, or that they serve a different purpose and are intended to be used by different categories of users... As we have learned from experience, particularly when designing document structures, there is usually not a single way to describe things and sometimes there are no compelling reasons to decide whether one particular way should be considered better than another. Semantic applications only make it worse, since there may be several ways to speak about the same thing. It appears to be necessary to take into account multiple perspectives.

1. China Toughens Its Restrictions on Use of the Internet, New York Times, December 29, 2012 ↩
2. Dismantling Utopia: How Information Ended the Soviet Union, by Scott Shane, Chicago: Ivan R. Dee, 1994, 324 pp.] ↩