

The Politics of Cyberspace (3): Disintermediation versus Confidentiality

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

The completely revised IS407 “Politics of Cyberspace” <
<http://www.mekabay.com/courses/academic/norwich/is407/index.htm> > course that started in
January 2011 included a module of references about WikiLeaks < <http://wikileaks.info/> > and the
role of disintermediated news gathering and distribution <
http://www.mekabay.com/courses/academic/norwich/is407/is407_resources/is407_week_08_link_s.htm >
> that may interest readers who are thinking about confidentiality of business affairs in the age
of the Internet.

For historical perspective, the students were able to read a 2003 interview with Daniel Ellsberg
discussing a report in *The Observer* of London <
<http://www.guardian.co.uk/world/2003/mar/02/usa.iraq> > about what *On the Media* (OTM)
director Brooke Gladstone described as “the scoops that the U.S. National Security Agency had
wiretapped several officials at the U.N. whose nations would be crucial votes on whether to support
an invasion of Iraq. A leaked report suggest that Angola, Cameroon, Chile, Bulgaria, Guinea, and
Pakistan were bugged, presumably the give the U.S. a leg up in precarious negotiations where few
votes for war can be entirely relied upon.” <
<http://www.onthemedial.org/transcripts/2003/03/14/03> > Gladstone commented that the story
was ignored by the established news media in the US.

In 2006, OTM co-host Bob Garfield discussed pressures by the Sunlight Foundation <
<http://sunlightfoundation.com/> > to make “government transparent & accountable.” In that year,
the House of Representatives in the US Congress “approved two measures to combat so-called
earmarks, the pet projects slipped into spending legislation.... One rule change requires House
members to put their names on the earmarks they propose. The other is a bill, already approved in
the Senate, that would create a public, searchable Web database of all federal grants and contracts.
That bill was introduced in the spring but then was secretly put on hold by a couple of senators,
preventing it from a full vote.” < <http://www.onthemedial.org/transcripts/2006/09/15/07> >
Citizen action removed the secret hold: “In a rare show of unity, a coalition of liberal and
conservative blogs asked readers to call their senators and find out if they had imposed the hold.
Volunteers managed to narrow it down to four possible culprits, at which point Republican Ted
Stevens stepped forward and claimed responsibility.” Garfield noted that the pressures for openness
by politicians “change the behavior of citizens in this what-does-one-vote-do culture. The idea of
actually holding representatives accountable seems to suggest opportunities for actually an engaged
electorate[.]”

The Sunlight Foundation also participated in a movement to track how members of Congress spend
their time. < <http://www.onthemedial.org/transcripts/2007/03/09/05> > Another project was an
organized database of government contracts showing exactly which organizations receive how much
money from US taxpayers. < <http://www.onthemedial.org/transcripts/2009/01/16/07> >

A March 2009 interview with WikiLeaks principal Julian Assange <<http://www.onthemediamedia.org/transcripts/2009/03/13/04>> challenged Assange on “if hypothetically he would publish information sent to his website that could lead to the deaths of innocents, such as, for instance, how to release anthrax into a town’s water supply.” Assange replied, “Yes, even if there is a possibility that it would lead to loss of life. It’s hard to imagine a circumstance where we would get a document and us not publishing it would be helpful. If they were ill motivated, then they could send that in private to terrorist groups, to neo-Nazi organizations, and those organizations could then develop their plans out of the sunlight. And that’s the greatest harm.” Bob Garfield pointed out that Assange “declined to provide your telephone number to our producers, or your whereabouts, for that matter.” Assange explained, “We are a bit cagey about some of our communications. The reason is that we deal with intelligence forces every day. If too much is known about the journalists that are working with us, their telephone can be tapped and monitored, and forces that are communicating with them can be monitored. The results of a slip-up on our behalf could be fatal to some of the people that we work with, so we’re very cautious to make sure that people can’t get at our sources by obtaining our telecommunications records.” Students in IS407 commented on the irony of secrecy by an organization touting openness.

In a May 2010 show, Bob Garfield interviewed Gabriel Schoenfeld, author of *Necessary Secrets: National Security, the Media, and the Rule of Law* <<http://www.amazon.com/Necessary-Secrets-National-Security-Media/dp/0393339939/>>, who argues strongly for limits on the publication of state secrets. Schoenfeld summarized his position at the end of the interview as follows: “I think the government can and should prosecute journalists who trespass on the public’s right not to know. And the public’s right not to know is something that’s rarely spoken about, let alone defended, but it’s perfectly obvious why we don’t want to know certain things that our government is doing. It’s because if we know those things, our adversaries know them as well.”

More on the issue of disintermediation and confidentiality in the next article.

* * *

M. E. Kabay, <<mailto:mekabay@gmail.com>> PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc. <<http://acsi-cybersa.com/>> and Associate Professor of Information Assurance <<http://norwich.edu/academics/business/infoAssurance/index.html>> in the School of Business and Management <<http://norwich.edu/academics/business/faculty.html>> at Norwich University. <<http://www.norwich.edu>> Visit his Website for white papers and course materials. <<http://www.mekabay.com/>>

Copyright © 2011 M. E. Kabay. All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.