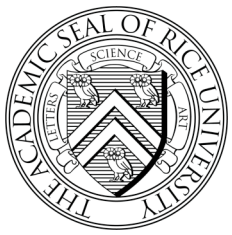

The James A. Baker III Institute for Public Policy
Rice University

Wiretapping, Surveillance and the Internet

BY

Christopher Bronk, Ph.D.
Fellow in Technology, Society and Public Policy
James A. Baker III Institute for Public Policy
Rice University

January 18, 2008

"Ways may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."

— Louis Brandeis, dissenting opinion, *Olmstead v. United States* (1928)

After a recent lecture covering the issues of online privacy and electronic monitoring, I asked the students of my information technology seminar to consider the balance between the need for national security versus the desire for individual privacy. The essays I received held a wealth of opinion on one of the most controversial issues for the current administration: the mass monitoring of telephone and electronic communications by government outside the conditions of a judicial warrant.

Educated by 1960s vintage Ph.D.s willing to pass along their views of government activities — and abuse — chronicled in the reports of the Church Committee, I expected a stream of outrage regarding the possibility that many or most of our telephone calls, e-mails and Internet habits might be viewed by the United States Intelligence Community. Instead, I received many replies in this vein: "For my part, I have nothing to hide from the government; my daily activities, e-mails, and travels show no evidence of suspicious activity. If the government chooses to watch me closely, I do not feel threatened."

Such a sentiment not only disregards the hard-won freedoms Americans consider sacred, but also reinforces an attitude within government that such freedoms have necessarily become obsolete. Under our system of government, anonymity and privacy are inextricably linked, because anonymity protects us from intimidation and coercion, no matter how subtle. We are a nation that casts our ballots anonymously, and for good reason. If unchecked, government-sanctioned eradication of anonymity will produce a chilling effect on political speech in this country.

In his remarks at a geospatial intelligence conference in San Antonio last October, Donald Kerr, the principal deputy director of national intelligence, gave insight into the government's perspective on the balance between security and privacy. Kerr asserted that we could have both, but retaining them would require jettisoning anonymity. "In our interconnected and wireless world, anonymity — or the appearance of anonymity — is quickly becoming a thing of the past,"

Kerr said, advocating the need "to move beyond the construct that equates anonymity with privacy. … Protecting anonymity isn't a fight that can be won." he quipped. As far as safeguarding this new definition of privacy, Kerr basically said, "Trust me."

But why is anonymity a lost cause? In part, it is due to our digital personae. We can blame the death of anonymity on credit cards, digital telecommunications, Google, the global positioning system, the National Security Agency (NSA) and a plethora of other phenomena. In becoming digital, our society has mapped more and more of its interactions to a format that is easily monitored, read and processed. Sure, we have gotten convenience in the deal, but Visa, MasterCard and American Express know what we buy. Over time, private companies and government agencies have compiled massive quantities of data produced by our ever-growing digital footprints. It should come as no surprise that the NSA is trying, according to CNN, "to create a database of every [telephone] call ever made."

The chief concern was expressed by another student: "My only worry is what the government constitutes as an attack on America. With 'terrorism' and 'national security' being used completely out of context these days, the government may unlawfully arrest someone as a 'terrorist who is putting national security at risk' when the individual may be doing nothing more than protecting America's citizens by revealing certain truths." While this fear may not yet be grounded, there is a valid concern regarding misuse of data collected by either government or commercial entities. ChoicePoint, an Atlanta-based data aggregation company, may be considered a private intelligence agency of sorts. Disturbingly, the company sold mountains of personal data to unscrupulous entities, which later used it to conduct thousands of cases of identity theft.

While data theft/loss and monitoring are obviously not the same, the concern is that monitored data will be inappropriately shared, mishandled or misused. Tremendous temptation exists to employ intelligence products for political or financial gain. By broadening our electronic dragnet to all communications, we open our system to unfathomable potential for abuse. For intelligence officials, who are, above else, charged with monitoring the activities of foreign persons, to declare anonymity dead, is frightening. It is worth remembering that the drafters of "The

Federalist Papers," Alexander Hamilton, James Madison and John Jay, shared their ideas on our system of government via an anonymously published pamphlet. When he wanted to communicate the potential threat of the Soviet Union, George Kennan submitted an article to *Foreign Affairs* that was attributed to X. By accepting unfettered digital monitoring by government, we open the door to a dim future marked by suspicion, distrust and paranoia. We do not want *Thoughtcrime*. Trust me.