

Eavesdropping in America, and even in Winsted?

In 2001, President Bush authorized the National Security Agency to bypass the Constitution and monitor our domestic phone calls and e-mails without a court order. This executive action was based on an Oct. 23, 2001 Justice Department memo by deputy assistant attorney general John Yoo to Alberto Gonzales. The action bypassed warrants required by the Foreign Intelligence Surveillance Act (FISA) and the Fourth Amendment protections in the Constitution.

The public was not aware of this action until December 2005, when the New York Times first reported that President Bush had authorized the National Security Agency (NSA) to eavesdrop secretly for years on the calls and e-mails of American citizens. Americans of all political persuasions were shocked by the announcement.

The FISA law was a compromise adopted in 1978 after Watergate and the discovery that innocent Americans were spied on for decades. To establish a balance between executive power to fight foreign spies with legal safeguards to protect Americans' privacy and liberty, Congress created a secret FISA court to review government requests for surveillance warrants. This law provided that FISA would be the exclusive means for monitoring domestic electronic communications. The law also stated that warrantless domestic wiretapping is a crime.

The FISA law reduced the Fourth Amendment standard required in ordinary criminal warrants — "probable cause" that a crime has been committed — to probable cause that the target is a foreign power or foreign agent. It kept in place the requirement that a judge review the warrant before it was executed.

On April 3, 2008, The New York Times reported that the administration has acknowledged that spying on citizens was not within the scope of its executive power and that FISA court review of the NSA program is required — after seven years of illegal spying on Americans!

The administration changed its position on this one aspect of domestic spying. But this reversal did not end the controversial warrantless surveillance. There are more deeply hidden examples of inappropriate and unconstitutional spying such as the disclosures that National Security Letters (NSLs) have been deceptively and illegally used by the FBI to spy on Americans.

On yet another front, private telecommunications companies assisted

within what one source described as "the largest database ever assembled in the world."

This may remind you of the discredited Total Information Awareness (TIA) program run by former Iran-contra felon John Poindexter that Congress defunded after a public outcry. Aspects of TIA migrated to other agencies, including the NSA. You

The Civic Beat

CHARLENE LAVOIE

may not mind data mining's typical approach — analyzing vast quantities of information instead of targeting based on individualized suspicion — when used by private companies such as Amazon.com to predict that a book will interest you based on your purchasing patterns. It is more problematic when secretly used to stigmatize you, deny you benefits or services, criminalize you by taking your actions out of context or, when combined with other databases, constitute what is effectively a warrantless search.

Does data mining work? A report by the nonpartisan Congressional Research Service noted data mining's limitations in counterterrorism, including issues such as data quality, mission creep (e.g., from counter-terrorism to tax collection or fighting crime generally), human errors in interpretation, terrorist-incident data sets too small to be useful as valid predictive models, false positives and privacy concerns.

There are now reportedly more than 200 data mining programs scattered throughout U.S. government agencies. These programs raise many issues, not the least of which are the loss of independent checks and balances and the curtailing of the Fifth Amendment presumption of innocence, resulting in privacy invasion and control over our own intimate information.

It is in the context of the national trend of spying on Americans that we look at what is going on in Winsted. The Aurora Estates developer, Anthony Silano, hired and posted "a team of private investigators" to keep "tabs on local land use board members for months." Mr. Silano proudly stated that he has employed this tactic for "similar purposes" in 2005 and 2006.

Selectman Michael Hamm, an avowed supporter and vocal advocate of Mr. Silano at public meetings and

behind the scenes, when asked for a comment on the Silano spying tactic cheered, "Good for him." Mr. Hamm subsequently commented that if the people being spied on "have to look over their shoulders, it implies some kind of guilt" and "if you've got nothing to hide, you've got nothing to worry about."

Mr. Silano's anti-social, uncivil tactics are reprehensible — one citizen labeled it "creepy." But where are our leaders? There is a total disregard of citizen concerns and profound lack of leadership in responding to the inappropriate comments of an elected official. The silence reveals much about these so-called "leaders."

Never mind that promoting spying on local citizens is an outrageous position for an elected official to take. Let's examine Mr. Hamm's comment that "if you've got nothing to hide, you've got nothing to worry about." This philosophy is completely opposite to the American understanding that we protect privacy for any reason, or no reason. Simply put, Americans prize privacy and want to keep it.

The "nothing to hide" argument stems from a faulty premise that privacy is about hiding a wrong. It considers privacy as a form of concealment or secrecy. Those advancing the "nothing to hide" argument have in mind a particular kind of visceral privacy harm, one where privacy is violated only when something deeply embarrassing or discrediting is revealed.

But even surveillance of legal activities can inhibit people from engaging in them.

Certain people will not be chilled by surveillance — indeed, probably most people here will not be. But, the value of protecting against such chilling is not measured only in terms of the value to those particular individuals. Chilling effects harm society because, among other things, they reduce the range of viewpoints being expressed and the degree of freedom with which to engage in political/community activity. Whether national or local, spying on citizens is just wrong. Mr. Hamm needs a civics lesson, to include a primer on privacy and how dearly it is held by the American people, even those who don't have anything to hide.

Charlene LaVoie is the community lawyer in Winsted. Her office is funded by the Shafeek Nader Trust for the Community Interest.

the NSA in spying on Americans. Court documents confirm that these companies allowed the NSA to tap directly into undersea cables and fiber optic cables that enable real-time backdoor access to these blurred domestic and international phone, e-mail, VoIP, and instant-message communications. The companies have engaged in data mining millions of intercepted American communications.

Data mining is increasing in government and business and it involves automated review of significant quantities of data to discern patterns and predict and influence behavior. Data mining assumes the patterns identified can highlight terrorist communications, as distinguished from ordinary communications, in addition to allowing more detailed searches