FACT SHEET IN OPPOSITION TO 06-S 2450 AND H-7525,
AN ACT RELATING TO PUBLIC UTILITIES AND CARRIERS

In the past few months, there has been justifiable outrage across the country surrounding revelations about the Bush Administration's wholesale invasion of citizens' privacy in numerous ways, including the collection of millions of telephone customers' calling records without consent or court order. One of the responses from the Bush Administration has been to discuss investigating journalists who have received information from government whistleblowers about these and other questionable administration activities. Amazingly, the R.I. General Assembly, rather than condemning these actions, is poised to pass legislation that would *actually legalize them* at the state level. The companion bills that would do this are S-2450 and H-7525. Both bills are pending in House Judiciary Committee, and one of them has already passed the Senate.

The two-page bill, at first blush, might seem rather modest. The one-sentence explanation given for the bill is that it would "provide law enforcement officials with the authority to obtain noncontent information from internet service providers pursuant to an administrative subpoena authorized by the superintendent of state police or the attorney general." This explanation, however, fails to indicate the true nature of the bill's scope, which also gives police access to customer telephone calling information and sets no standards for the issuance of a subpoena.

Just compare the bill with what has happened nationally in recent months:

* The National Security Agency asked telephone companies to turn over customers' calling information, without either customer consent or court approval. This bill would likewise authorize state and local police and the Attorney General to obtain that same information merely by issuing an administrative subpoena – without customer knowledge or court oversight.

* The U.S. Attorney General has stated an interest in investigating journalists who have reported on information provided them by government whistle-blowers. This bill would allow state and local police and the Attorney General to obtain the records of all phone calls made to and from a journalist merely by issuing an administrative subpoena – without the reporter's knowledge (or that of the people she has called) or court oversight.

* The U.S. Attorney General has expressed an interest in requiring major Internet service providers and search engines like Google to maintain data about the web sites that customers visit so that the government can gain access to those records. Earlier this year, the government actually subpoenaed Google to hand over millions of such records. This bill could potentially authorize state police and the Attorney General to seek such information.

There are a few key points to emphasize about S-2450/H-7525. First, as noted above, although it has been touted only as providing police access to Internet subscriber information, the bill also gives the police access to telephone information, including the phone numbers that a particular subscriber called or received calls from. Second, as explained more fully below, the "administrative subpoena" process provides absolutely no standards or safeguards, and gives police carte blanche authority to obtain both phone and Internet information at will on anyone they choose.

* As a substitute for the warrant process, administrative subpoenas circumvent all of the usual safeguards in place before law enforcement officials can obtain information or evidence about a person or crime. Instead of having to go before a neutral magistrate who would independently determine that

sufficient grounds exist to invade a person's privacy, the administrative subpoena process leaves everything in the hands of the police themselves, without any oversight.

* Unlike a warrant, the bill also does not require the police to have probable cause in order to issue an administrative subpoena. In fact, in order to obtain a customer's information under the bill, police do not need to have probable cause that a crime has been committed, they do not need to have probable cause that the search will turn up evidence of a crime, and they don't need to have probable cause that the person whose information is being sought is even a suspect in a crime! The investigation can be for any reason and for *any* criminal violation – from a petty misdemeanor to a capital crime.

* Ultimately, the bill is touted as one of convenience to police, because seeking a warrant can be burdensome and time-consuming. As for the burden, police must obtain warrants to search for evidence for the most serious of offenses and, when necessary, judges sign warrants expeditiously. Convenience to law enforcement should not be the grounds for overriding fundamental procedural safeguards designed to preserve people's privacy.

* The administrative subpoena process not only provides the person whose information is sought no opportunity to contest the subpoena, he or she is not even made aware that the information has been provided to police.

* In many instances, use of administrative subpoenas in this context will not get police the information they are seeking. As police officials have testified, there are many cases when e-mail messages cannot be traced at all (such as instant messaging), some Internet service providers do not keep records of use that are retrievable, and those that do usually keep it for a sufficient period of time that a warrant would suffice. It also remains unclear how quickly ISP's are able to respond to administrative subpoenas in any event, so the investigatory impact on circumventing the warrant requirement may be minimal.

* Although the bill limits police to obtaining "non-content" Internet information, the federal government has begun arguing that access to URL information (web site addresses) is "transactional" information and not content information, and therefore accessible to them. The bill also allows police to obtain access to customers' credit card and bank account information.

Concerns about misuse of data like this are hardly abstract. Last year, in an analogous context, Woonsocket police ran through a federal database the license plate numbers of cars parked at a political event. We learned last December that in 2004, local law enforcement authorities notified the Department of Defense of a peaceful political protest at a National Guard recruiting station in Providence. And the State Police, the primary proponents of this bill, have vigorously opposed legislation sponsored by Rep. Edith Ajello that would restrict police from engaging in political surveillance.

Passage of S-2450 and H-7525 at any time would raise serious privacy concerns. Approval of legislation at this particular time, in light of the disclosures that have taken place in recent months at the national level, would be especially unfortunate. The RI ACLU urges concerned residents to contact their state Representative and urge their opposition to this troubling bill.