court whose communications are going to be monitored. And it can do this even if some or all of the people it's targeting are communicating with innocent people *inside* the U.S.

- **The law allows the government to intercept U.S. citizens' and residents' international telephone and email communications without having to identify the facilities, phone lines, email addresses, or locations to be monitored.**

The government doesn't need to tell the FISA court whose communications it intends to monitor, and it doesn't need to tell the court which phone numbers or email addresses (or communications lines, or gateway switches) it intends to monitor, either. Nor does it even need to tell the court which telecommunications company it is demanding access to. In fact, the new law allows the government to conduct intrusive surveillance without ever telling the court who it intends to surveil, what phone lines and email addresses it intends to monitor, where its surveillance targets are located, or why it's conducting the surveillance. To conduct surveillance under the law, the government need only to tell the court that its targets are outside the U.S. (even if they're communicating with people *inside* the U.S.) and that a "significant purpose" of the surveillance is to collect foreign intelligence information. By allowing the government to conduct surveillance without identifying the specific surveillance targets and specific facilities to be monitored, the new law permits the mass acquisition of U.S. citizens' and residents' international communications. Theoretically, the government could use the new law to collect all phone calls between the U.S. and London, simply by saying to the FISA court that a significant purpose of its new surveillance program is to collect foreign intelligence information.

- **The law allows the government to conduct intrusive surveillance without meaningful judicial oversight.**

The new law gives the FISA court an extremely limited role in overseeing the government's surveillance activities. The FISA court does not review individualized surveillance applications. It does not consider whether the government's surveillance is directed at agents of foreign powers or terrorist groups. It does not have the right to ask the government who, what, where, or why it is inaugurating any particular surveillance program. Under the new law, the FISA court's role is limited to reviewing the government's "targeting" and "minimization" procedures. And even with respect to the procedures, the FISA court's role is to review the procedures at the *outset* of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time. Even at the outset of a new surveillance program, the government can initiate the program without the court's approval so long as it submits a "certification" within seven days. In the highly unlikely event that the FISA court finds the government's procedures to be deficient, the government is permitted to continue its surveillance activities while it appeals the FISA court's order. *In other words, the government can continue its surveillance activities even if the FISA court finds those activities to be unconstitutional*.

- **The law places no meaningful limits on the government's retention and dissemination of information relating to U.S. citizens and residents.**

Thanks to this new law, there is no question that thousands or even millions of U.S. citizens and residents will find their international telephone and e-mail communications swept up in surveillance that is "targeted" at people abroad. Yet the law fails to place any meaningful limitations on the government's retention and dissemination of information that relates to U.S. citizens and residents. The law requires the government to adopt "minimization" procedures – procedures that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." However, these minimization procedures must accommodate the government's need "to obtain, produce, and disseminate foreign intelligence information." In other words, the government will be able to retain or disseminate information about U.S. citizens and residents so long as the information is "foreign intelligence information." Because "foreign intelligence information" is defined broadly (as discussed below), this is an exception that swallows the rule. In addition, *nothing in the law prevents the government from compiling huge databases of foreign intelligence information and searching those databases later for information about U.S. citizens and residents*. Once the government acquires the communications of U.S. citizens and residents (through surveillance that is "targeted" at people located outside the U.S.), nothing in the law precludes the government from searching these databases – even with searches that are targeted at U.S. citizens and residents – and reviewing the content of individual communications.

- **The law does not limit government surveillance to communications relating to terrorism.**

The new law allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather "foreign intelligence information." There are multiple problems with this. First, under the new law the "foreign intelligence" requirement applies to entire surveillance programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications – not only those that relate to foreign intelligence. Second, the phrase "foreign intelligence information" has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the "foreign affairs of the United States." Journalists, human rights researchers, academics, and attorneys *routinely* exchange information by telephone and e-mail that relates to the foreign affairs of the U.S. (Think, for example, of a journalist who is researching the "surge" in Iraq, or of an academic who is writing about the policies of the Chávez government in Venezuela, or of an attorney who is negotiating the repatriation of a prisoner held at Guantánamo Bay.) The Bush administration has argued that the new law is necessary to address the threat of terrorism, but the truth is that the law sweeps much more broadly and implicates all kinds of communications that have nothing to do with terrorism or criminal activity of any kind.

- **The law gives the government access to some communications that are purely domestic.**

The new law prohibits the government from "intentionally acquiring any communication as to which the sender and all intended recipients are *known at the time of the acquisition* to be located in the United States." The government itself, however, has acknowledged that, particularly with email communications, it is not always possible to know where the parties to

the communication are located. Under the new law, the government can acquire communications so long as there is uncertainty about the location of the sender or recipient. A reasonable law would have required any uncertainty to be resolved in favor of the privacy rights of U.S. citizens and residents, but this law requires uncertainty to be resolved in favor of the government. Thousands or even millions of purely domestic communications are likely to be swept up as a result.

- **The law immunizes the telecoms that participated in the Bush administration's warrantless wiretapping program.**

In addition to investing the executive branch with sweeping new surveillance powers, the new law immunizes the telecommunication corporations that facilitated the warrantless wiretapping program that the National Security Agency operated between 2001 and 2007. Telecommunications corporations that violated the law and allowed the government to trample the privacy rights of thousands of Americans should be held accountable for their activities. Letting them off the hook only invites more abuses in the future.