

By Gary S. Lincenberg and Benjamin N. Gluck

A Patriotic Critique of the PATRIOT Act

The antiterrorism legislation that Congress passed in haste is a threat to civil liberties

In his famous dissent in a wiretap case, Justice Louis Brandeis wrote, “Experience should teach us to be most on guard to protect liberty when the Government’s purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.”¹

Brandeis’s words have special significance today. The U.S. Justice Department, under Attorney General John Ashcroft, is using September 11 as cover for the most aggressive expansion of law enforcement authority in years. To show unity in the fight against terrorism, Congress passed the USA PATRIOT Act. PATRIOT is an acronym for the act’s title, “Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.” Afraid to dissent lest they be viewed as not rallying around the flag, legislators passed the PATRIOT Act with little debate. A full and healthy debate surely would have weeded out those parts of the act that needlessly encroach on civil liberties. Despite its title, the act generally will be employed in cases having little to do with terrorism. Thus it should be judged primarily as a crime control measure.

The PATRIOT Act significantly expands the authority of law enforcement to invade privacy without meaningful judicial oversight. For example, Section 216 of the act allows law enforcement officers to access electronic communications simply by certifying to a federal judge that the records of a person’s electronic communications are “relevant to an ongoing criminal investigation.” The judge then must issue an ex parte order giving law enforcement access to the person’s “dialing, routing, addressing, and signaling information.”

Proponents of the act note that this standard is no more lenient than one needed to trap and trace a list of dialed telephone numbers. But Section 216 permits law enforcement to record and review a list of all the Internet sites a person visits. Accessing a list of Internet sites reveals much more than a list of telephone numbers. Internet sites reveal content. Yet this search of a person’s Web interests permitted under Section 216 is not subject to any kind of judicial review. Nor is it limited to terrorism or national security investigations.

The PATRIOT Act also permits the government to delay notifying the subject of a search that a search has taken place. Under this rule, if a court finds “reasonable cause to believe” that immediate notice would adversely affect the investigation, the government may delay notice for a “reasonable period.” The reasonable-cause-to-believe standard will be easy to satisfy—and easy to abuse. “Sneak and peek” warrants may eventually become the rule rather than the exception, since the new provision applies not just to terrorism investigations but to all crimes. For years, the notification requirement has

permitted people to seek timely judicial review of unlawful searches. Now, many of these searches simply will be kept secret during the pendency of investigations, which often drag on for years.

The PATRIOT Act’s expansion of control measures for money laundering also goes too far. Money laundering statutes can be effective tools to combat crime. Congress and prosecutors must be careful, however, not to lump unknowing persons who end up with “dirty money” together with those who perpetuate the unlawful activities that generate it. Even as the U.S. Sentencing Commission has begun to recognize that the penalties for money laundering are often disproportionate to the underlying crimes upon which the laundering charges are predicated, the PATRIOT Act greatly expands not only the unlawful activities within the scope of the money laundering statutes but also the statutes’ foreign jurisdictional reach and the related regulatory reporting requirements.

The act puts much of the onus on banks to root out money laundering at the expense of consumer privacy. For example, the act obligates banks to take greater steps to verify the identification of customers before they open accounts. When the government tried to promulgate a similar requirement in 1999, it backed down after receiving thousands of adverse comments from consumers who did not want their financial privacy invaded. In the wake of September 11, however, this rule passed with little fanfare.

While financial institutions already must comply with extensive requirements to report suspicious activities, the act adds more. The act immunizes financial institutions from liability for overreporting while penalizing them for underreporting. Naturally, financial institutions will err on the side of filing reports and will no doubt report many innocent activities. Persons who have done nothing wrong generally will not know that banks and the government have placed their names and information in suspicious activity files—and these files will follow the blameless parties throughout their lifetimes.

The events of September 11 do not justify changing the balance between government intrusion and civil liberties outside the arena of national security and terrorism. If Congress felt the need to act quickly by passing antiterrorism legislation, it should have tailored the PATRIOT Act more narrowly. This would have alleviated its spillover into general criminal law enforcement and helped avoid unnecessary governmental overreaching. ■

Gary S. Lincenberg is a partner and Benjamin N. Gluck is an associate with Bird, Marella, Boxer & Wolpert. They specialize in white collar criminal and enforcement matters.

¹ Olmstead v. United States, 277 U.S. 438 (1928).