9·11 사건 이후 美國 國土安保法制의 변화

박 훤 일 (경희대 법대 교수)

차 례

최근 들어 미국 비자 얻기가 어려워졌다. 특별한 예외가 없는 한 미국 영사와 미리 예약하고 면담을 해야 하며, 유학생의 경우에는 유학생 신상정보 시스템(SEVIS)이 설치된 각급 학교에서 발급한 입학허가서(I-20 Form)를 반드시 소지해야 미국에 들어갈 수 있다. 그리고 방문/관광 비자로 입국한 경우에는 학생 비자로의 변경이 일체 허용되지 않는다.

8월 초부터는 미국 비자가 없는 외국인 승객이 미국 공항에서 비행기를 갈아타는 것도 일시 중단되고 있는데, 이 조치는 미 본토에 대한 테러위협이 존재하는 한 계속 시행될 것으로 보인다. 2002년 새로 제정된 「국경보안 및 비자 개혁법」에 따라 2004년 10월부터는 입국자 전원의 비자에 생체인식(biometrics) 정보가 수록될 예정이다.

---

1. 머리말

9·11 사건 이후 미국이 근본적으로 바뀌어 가고 있다. 앞에서 살펴본 사례는 외국인으로서 겪게 되는 표면상의 변화에 불과하다. 2001년 9월 11일 미국의 심장부인 뉴욕 맨해튼의 무역센터 빌딩과 워싱턴 국방부청사가 테러 공격을 받고 막대한 피해를 입은 사실은 미국의 정보력과 첨단기술에 대한 자신감을 무너뜨리고 국토방위에 대한 경각심을 불러일으켰다.

이를 계기로 미국은 국토안보를 위한 조직을 대대적으로 정비하는 한편 애국법, 사이버보안강화법 등 새로운 법률을 제정하여 제2의 테러 방지에 만전을 기하고 있다. 본고에서는 우리나라에도 직·간접의 영향을 미치고 있는 사이버공간(cyberspace)의

안전을 위한 미국 법제상의 변화를 살펴보기로 한다.

2. 사이버 보안의 중요성

미 국내선 여객기를 납치하여 테러를 감행한 알 카에다 조직원들은 미국내 비행학교에 유학을 온 뒤 비행기 조종술을 익히고 합법적인 신분을 취득하여 테러 공작을 준비한 것으로 알려졌다. 그리고 중동의 테러 단체 조직원들은 공공연하게 인터넷을 지하드(聖戰)에 이용하고 있다. 문명의 첨단이기가 무고한 사람들을 살상하는 테러에 활용되고 있는 것이다.

이들 테러 단체는 인터넷 상의 각종 암호기술과 소프트웨어를 이용하여 테러 목표와 공격방법에 관한 지시를 조직원들에게 전달하고 있다고 한다. 사전에 조직원들이 인터넷 상에서 암호기술 및 암호해독 소프트웨어를 공유한 뒤 테러 공작과 관련된 정보를 일반에 공개된 채팅룸이나 포르노사이트를 이용하여 교환하고 있다는 것이다. 특히 오사마 빈 라덴은 2000년 미 정보당국이 아프가니스탄의 은거지로부터 송출되는 위성통신을 감청한다는 사실을 눈치채고는 연락수단을 암호화된 인터넷 통신으로 대체하였다고 한다.[1)]

이에 따라 미국 정부는 물리적인 테러뿐만 아니라 화생방 및 사이버 공격에 대비하기 위한 종합적인 대응전략을 모색하고 있다. 그 중에서도 정보기술(IT)의 비약적인 발전에 따라 사이버 테러에 대한 대책마련에 부심하고 있다.

3. 국토안보를 위한 조직 정비

종래 미국은 국가안전보장, 기반시설보호, 테러 대응을 위해 대통령 직속의 국가조정자(National Coordinator)라는 직책을 설치하였으나 그 권한과 책임이 모호하여 법무부, 연방수사국(FBI), 연방긴급재난관리국 등의 기능과 혼선을 빚게 되었다.

이 과정에서 9·11 테러 사건이 발생하자 대통령실(Executive Office of the President)에 對테러 업무총괄기구인 국토안보국(Office of Homeland Security)을 서둘러 설치하고, 테러 위협·공격과 관련된 정책을 수립하는 국토안보회의(Homeland Security Council), 주요기반시설을 운영하는 민간부분과의 협력 강화를 위한 사이버공간 담당 특별보좌관(Special Advisor to President for Cyberspace Security), 정보통신기반시설을 보호하기 위한 국가기반자문회의(National Infrastructure Advisory Council)와 주요기반보호협의회(Critical Infrastructure Protection Board) 등을 신설

1) 장 완, 「사이버범죄의 보안대책-암호정책을 중심으로」, 한국형사정책연구원 연구보고서 01-17, 2001, 7~8면.

또는 확대 개편하였다.[2)]

이러한 조직은 대통령행정명령(Presidential Decision Directive: PDD)에 의거하여 신설·개편되었으며, 민간부문 및 주 정부와의 협력, 정보공유, 종합적인 대응을 강조한 것이 특색이다. 2002년 11월에는 마침내 장관급인 국토안보부(Department of Homeland Security)로 격상되어 각 부처별로 산재되어 있던 기구 및 조직을 통합하였다.

국토안보부의 주요 임무는 ① 미국내 테러 공격의 방어, ② 테러에 대한 미국내 취약점 개선, ③ 테러 공격 시 신속대응 및 피해의 최소화 등이다. 구체적으로는 국경·통신 보안, 비상대응체제, 화생방·핵 대응방안, 정보분석 및 기반보호를 위한 직제를 두고 있다. 국경 및 해안경비, 이민 업무가 국토안보부로 이관되었으며, 사이버공간의 보안 역시 국토안보부가 관장하게 되었다. 미국의 금융·에너지·행정·교통시설 등 주요기반분야가 정보통신시스템과 네트워크로 연결되어 있으므로 만일 사이버 공격이 감행될 경우에는 서비스 장애는 물론 공공의 안녕질서와 국민경제에 대한 엄청난 지장을 초래하게 될 것이다. 이에 따라 FBI 산하의 국가기반보호센터(National Infrastructure Protection Center: NIPC) 등을 2003년 3월 1일자로 통합하고 사이버 공격으로부터 미국의 주요기반시설을 보호하는 데 우선순위를 두고 있다.

백악관은 2003년 2월 「사이버공간 안전을 위한 국가전략」(National Strategy to Secure Cyberspace)을 공표하고, 연방·주 정부, 민간기업과 국민 개개인에 대하여 사이버공간의 안전을 확보하기 위한 실천방안을 제시하였다.

4. 국토안보를 위한 법제 정비

9·11 사건에 대한 미국 정부의 법적 대응은 2001년 10월 테러 사건의 복구와 탄저병 살포로 어수선한 가운데 의회에서 통과된 「애국법」과 2002년 11월 「국토안보법」에 묻어서 통과된 「사이버보안강화법」 두 가지로 요약할 수 있다.

가. 애국법

9·11 테러 사건이 발생하자 정부와 의회는 초당파적인 대테러 법안을 마련하였다. 하원과 상원이 「Patriot Act」(H.R.2975)와 「USA Act」(S.1510)를 각각 가결함에 따라 두 법안은 양원의 통합·조정을 거쳐 하원과 상원을 통과하고 2001년 10월 26일 부시 대통령의 서명을 얻어 마침내 「USA Patriot Act」[3)]로 공포되었다.

---

2) 김현수, "9·11 이후 미국 국토안보정책 현황 분석-조직정비와 사이버보안 강화법제를 중심으로", 2002.

3) 입법과정에서 보았듯이 이 법은 상원의 Uniting and Strengthening America Act와 하원의 Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act를 합친 것으로 약칭 "USA

애국법은 기존 전기통신프라이버시법(Electronic Communications Privacy Act of 1986: ECPA)[4] 등을 개정하여 사이버 공격의 수사에 따른 절차 요건을 대폭 완화하고 수사기관(law enforcement authorities)의 권한을 강화한 것이 특색이다. 이 법은 2005년 12월 31일까지만 발효되는 한시법(sunset law)이다.

애국법은 다음과 같은 장, 절로 구성되어 있는데, 그 중에서도 사이버 보안을 위하여 마련된 기존 법률규정에 대한 특칙을 조항별로 해설한다.[5]

애국법의 내용

제1장 테러에 대한 국내안보(Domestic Security)의 강화
제2장 감시절차(Surveillance Procedures)의 강화
제3장 국제적인 돈세탁 금지 및 反테러 자금법
  제1절 국제적인 돈세탁 방지 및 관련조치
  제2절 예금비밀법 개정법률 및 개선방안
  제3절 통화범죄(Currency Crimes)
제4장 국경의 경비(Protecting the Border) 및 이민 규정
제5장 테러수사에 대한 장애의 제거
제6장 테러 피해자, 공안담당공무원 및 그 가족에 대한 지원
제7장 주요기반보호를 위한 정보공유의 강화
제8장 테러에 대한 형사법(Criminal Laws)의 강화
제9장 정보수집(Intelligence)의 개선
제10장 보칙

(1) 컴퓨터해킹 수사에 있어서의 감청권한(제202조)

기존 컴퓨터사기·남용금지법(Computer Fraud and Abuse Act: CFAA, 18 U.S.C. §1030)에 의하면 수사관은 동법의 위반 사항에 대한 유선통신(wire communications) 내용을 감청하기 위한 영장을 발부 받을 수 없었다. 애국법에서는 유선통신에 대한 감청영장을 발부 받을 수 있는 대상에 중범죄(felony violations)를 추가하였다.

(2) 음성메일 및 저장된 음성통신 획득(제209조)

Patriot Act" 또는 "애국법"으로 불린다.

4) 이 법은 여러 차례에 걸친 부분 개정에 이어 1996년 국가정보기반보호법(National Information Infrastructure Protection Act: NIIPA)으로 전면 개정되었다.

5) Lee M. Zeichner, *Cyber Security and Corporate Liability, Business Law Monographs Corporate Series*, Volume C10 Matthew Bender, LexisNexis, 2002, pp.7-15~21.

기존 전기통신프라이버시법(ECPA)에서는 저장된 e-메일 등의 전자통신(stored electronic communications)에 대한 접근은 수색영장으로 가능했지만 저장된 유선통신(음성메일 등)은 감청영장(wiretap order)이 있어야 했으므로 수사기관에 엄청난 절차상의 부담을 안겨줬다. 예컨대 수사대상의 전자우편함에 음성첨부물이 있는 경우에는 수색영장 만으로는 그 내용을 파악할 수 없었다.

애국법은 유선통신의 정의에서 유선통신의 '전자적인 저장장치'를 삭제하여 저장된 유선통신도 저장된 전자통신과 같이 접근할 수 있도록 했다.

(3) 전자적 증거에 대한 제출명령의 범위(제210조)

기존 전기통신프라이버시법 제2703조(c)항에서는 법집행기관이 제출명령(subpoena)만으로는 고객의 이름, 주소, 서비스 기간, 지급수단 같은 제한된 정보만 획득할 수 있었다. 따라서 범인이 가명을 사용하여 등록한 경우에는 실효가 없었다. 더욱이 동 조항은 주로 전화통신과 관련된 기술이 많아 컴퓨터 네트워크에서는 이를 적용하기 어려웠다.

애국법에서는 이 조항을 수정하여 법집행기관이 제출명령을 가지고 얻을 수 있는 기록을 신용카드 또는 은행계좌번호 등 용의자의 신원확인에 필요한 정보로까지 확대했다.

(4) 케이블법률 범위의 명확화(제211조)

종래 전화, 인터넷 서비스에 대하여는 전기통신프라이버시법, 감청법이 적용되고, 케이블 서비스에 대해서는 케이블법(Cable Act)이 적용되었는데 동 법은 케이블 회사가 보관하는 가입자의 기록에 대한 법집행기관의 접근을 극도로 억제했다.

사실 케이블이 케이블 방송뿐만 아니라 전화, 인터넷 서비스까지 제공하는 오늘날에는 범죄수사에 많은 제한이 따랐다. 따라서 고객이 케이블 회사로부터 인터넷 서비스까지 받는 경우에는 전기통신프라이버시법, 감청법 등의 공개 요건(disclosure requirements)에 따라 인터넷 서비스와 관련된 고객의 기록을 공개할 수 있도록 하였다.

(5) 통신회사에 의한 긴급공개(제212조)

종전에는 통신회사가 비상시에도 고객의 기록이나 통화내역을 공개(emergency disclosures)할 수 있는 근거규정이 없었다. 예컨대 어느 이용자가 테러공격을 모의하고 있다 할지라도 수사기관에 그에 관한 정보를 공개하면 민사소송을 당할 우려가 있었다.

이에 따라 애국법에서는 통신서비스제공자가 살인, 중대한 상해, 재산권에 대한 침해를 방지하기 위해서는 자발적으로 통신의 내용 또는 고객의 기록을 법집행기관에 공개할 수 있도록 하여 통신서비스제공자의 면책범위를 명시하였다.

(6) 전화이용상황 기록장치와 팬/트랩법(제216조)

1986년에 제정된 펜/트랩법(Pen Register and Trap and Trace Statute)은 주로 전화 등의 유선통신의 수집에 관하여 규율하고 있었으므로 컴퓨터 네트워크 통신에는 적용상의 문제가 있었다. 이에 따라 애국법에서는 펜/트랩 대상에 휴대전화번호, 인터넷사용자계정, e-메일주소, IP주소, 포트번호 등을 포함시켰다. 그러나 통신내용의 감청까지 허용하는 것은 아니다.

또한 종전에는 연방법원이 오직 당해 법원의 관할지역에서만 펜/트랩 장치의 설치를 허가할 수 있었으므로 여러 지역에 걸쳐 정보를 획득하기 위해서는 개개의 사업체별로 독립된 명령을 발부 받아야 했다. 그러나 애국법에 따라 영장집행의 효력이 확대하여 미국내의 어떠한 통신서비스제공자에 대해서도 지원을 받을 수 있게 되었다.

법집행기관이 인터넷 기타 통신서비스제공자에게 펜/트랩명령을 집행하는 경우 회사 스스로 필요한 정보를 수집하여 법집행기관에 정보를 넘겨줄 수 있어야 하므로 장치가 마련되어 있지 않은 경우에는 영장을 집행해도 효과가 없었다. 그러나 다음과 같은 특별보고서(special report)를 봉인한 상태로 30일 이내에 법원에 제출하면 수집이 가능하게 되었다. 즉, 펜/트랩장치(예컨대 FBI의 DCS1000 'Carnivore')를 설치·접근한 수사관의 성명, 장치를 설치·접근하고 제거한 일시, 장치의 설정 또는 변경 내역, 장치에 의하여 수집한 정보 등이다.

(7) 컴퓨터 침입자의 통신내용 감청(제217조)

컴퓨터 시스템 관리자가 시스템에 무단 침입하는 자(computer trespasser)를 감시하기 위하여 법집행기관의 지원을 받을 수 있도록 하였다. 가장 효과적인 방법은 법집행기관이 대상 컴퓨터 시스템에 전송되는 무단 침입자의 통신을 감청하는 것이다. 이를 위해 법집행기관에 소속된 조사관은 컴퓨터 관리자로부터 통신감청에 대한 동의를 얻어 감청하는 내용이 조사와 관련이 있다는 합리적인 근거를 가지고 침입자가 보내거나 수신하는 통신을 감청할 수 있다.

(8) e-메일 수색영장의 전국적 효력(제220조)

종전에는 개봉되지 않은 e-메일을 공개할 때 당해 지역을 관할하는 법원으로부터 6개월짜리 수색영장(search warrant)을 받아야 했다. 이러한 관행은 수사에 엄청난 지장을 초래하였으므로 애국법은 제출명령과 동일하게 수색영장을 사용할 수 있도록 하고 영장발부법원의 관할지역 밖에서도 e-메일 등에 대한 수색영장을 사용할 수 있도록 하였다.

(9) 사이버테러의 억제와 방지(제814조)

컴퓨터사기·남용방지법에서 보호되는 컴퓨터에 불법 침입한 자에 대한 형벌을 최

고 10년(초범의 경우)과 20년(상습범의 경우)으로 강화하고 이러한 불법침입자는 특정 유형의 침해행위를 요하지 않고 침해행위의 고의만 있으면 되도록 하였다. 국가안보 또는 사법절차에 사용되는 컴퓨터에 대한 침해행위는 피해액이 5천달러에 미달해도 범죄로서 규정하였다. 이 법에 의하여 보호를 받는 컴퓨터(protected computer)의 범위를 외국에 소재하더라도 미국에서의 주간(interstate) 또는 대외(foreign) 통상거래에 이용되는 컴퓨터까지 확대하였으며, 해외에서 범행을 하였더라도 미국 내에서 형사소추할 수 있도록 관할범위를 확장했다. 그리고 주법에서 컴퓨터 불법침입죄로 처벌받은 것도 전과(prior offenses)로서 취급하기로 했다.

(10) 정부의 요청에 따른 기록보존에 관한 민사소송상의 항변(제815조)

종래 전기통신프라이버시법에 의하여 민사소송을 당하는 경우 대배심의 제출명령(grand jury subpoena)이나 법정 사유 또는 계약상의 요건을 선의로 신뢰한 것이 항변사유가 되었다.

애국법은 선의로 신뢰한 것(good-faith reliance)이라는 법정항변(statutory defense) 사유에 증거를 보존토록 한 정부의 요청을 따르는 것도 포함시켰다.

(11) 사이버보안 포렌식[6] 능력의 개발 및 지원(제816조)

법무부장관이 적절하다고 인정하는 지역에 컴퓨터포렌식연구소(computer forensic laboratory)를 설치할 수 있게 하고, 기존 컴퓨터포렌식연구소에 대하여는 지원을 강화하고 특정 포렌식과 훈련능력을 제공하도록 하였다.

나. 사이버보안강화법

미국은 사이버공간에서의 보안을 강화하기 위하여 2002년 11월 25일 국토안보부(DHS)의 설치를 목적으로 하는 국토안보법(Homeland Security Act)에 사이버보안강화법(Cyber Security Enhancement Act)을 포함시켜 제정하였다.

이 법은 기존 컴퓨터사기·남용방지법(CFAA)과 관련 양형위원회(Sentencing Commission)의 가이드라인을 수정하고 컴퓨터 무단 침입자(computer trespasser)가 컴퓨터를 도구로 사용하여 고의로 생명·신체에 중대한 위해를 가하거나 가하고자 한 경우 중형을 과하도록 했다. 또한 국가기반보호센터(NIPC)가 정부 차원의 위협측정, 경보, 수사, 주요 기반시설에 대한 대응센터로서의 역할을 다할 수 있도록 그 기능을 강화했다.

그리고 통신서비스제공자(ISP)가 사람의 생명·신체에 대한 중대하고 급박한 위험

6) 컴퓨터포렌식(computer forensics)이란 컴퓨터 관련증거를 법정증거로 제출하기 위한 과학적인 증거수집 절차 또는 방법을 말한다.

이 우려되는 상황에서 지체없이 정보제공을 할 수 있는 '긴급시 공개'(emergency disclosure) 예외 규정의 범위를 넓혔다. 즉, 긴급을 요하는 경우 법원의 감독이나 이용자에 대한 고지 없이도 법집행기관과 전기통신의 내용을 공유할 수 있도록 한 것에서 한 걸음 더 나아가 ISP가 선의로(in good faith) 사람의 생명·신체에 중대한 위험이 우려되는 상황에서 지체 없는 정보의 공개가 요구된다고 믿은 때에는 정부기관에 대하여 관련 정보를 제공할 수 있도록 하였다. 요컨대 ISP의 정보공개 요건에 있어서 대상이 법집행기관이 아닌 정부기관으로 확대되고, 합리적인 확신(reasonable belief)이 아닌 선의의 신뢰(good-faith belief)로도 족하며, 생명·신체에 대한 급박한 위험이 아닌 단지 생명·신체에 대한 위험으로 충분하게 되었다.

종래 전기통신프라이버시법(ECPA)에서는 감청설비에 대하여 신문·잡지·광고지 기타 출반물에 의한 일정한 광고가 금지되었다. 사이버보안강화법에서는 기타 출판물에 전자적 수단에 의한 배포(disseminates by electronic means)를 추가하여 전자적 수단에 의한 감청설비의 광고를 규제하고, 광고를 하는 자가 광고의 내용을 인식할 것을 요구하였다.

또한 컴퓨터 범죄에 대한 처벌을 애국법보다 더 강화하였다. 즉, 사이버 공격자가 고의 또는 과실로 심각한 신체적 상해를 유발하거나 하고자 하는 경우 벌금 또는 20년 이상의 징역에 처하거나 병과하고, 사망케 한 경우에는 벌금 또는 징역, 최장 무기징역에 처하거나 이를 병과할 수 있도록 하였다.

전기통신프라이버시법에서는 ISP가 법원의 영장 등에 의한 통신감시·감청에 조력하는 경우 책임을 면제하였으나 사이버보안강화법은 법정 허가요건(statutory authorization)을 추가하여 이 요건만 충족하면 정부기관이 ISP에 대하여 정보제공이나 조력을 강제할 수 있도록 하였다.

5. 맺음말

미국이 9·11 사건 이후 테러리스트들이 미국 내에 잠입하는 것을 막기 위해 비자 심사를 강화하고 외국 유학생들을 철저히 감시하기로 하는 것은 어찌 보면 당연한 결과라 할 수 있다. 그러나 그 동안 미국이 전세계적으로 자유와 인권을 전파하고 프라이버시권을 강조하던 것에 비추어보면 크게 후퇴한 것이라는 느낌을 지울 수 없다.

이에 따라 미국의 재야 시민단체 등에서는 "미국인들이 자유를 잃어가고 있다"면서 미국의 기본권보장을 크게 후퇴시킨 애국법의 시행에 강력히 반발하였다. 예컨대 애국법 제215조에 의하면 법집행기관은 테러에 대한 수사를 이유로 도서관에서 누가 어떤 책을 대출했고, 서점에서 누가 어떤 책을 사갔는지, 또 누가 도서관의 컴퓨터로 인터넷에 접속하여 무슨 사이트를 검색했는지 자료제출을 요구할 수 있다. 게다가 사이

버공간에서는 법원 영장 등의 절차 요건을 대폭 간소화하고 수사기관이 각종 다양한 감시기술을 사용하여 수사할 수 있도록7) 하였으므로 정부당국이 마음만 먹으면 조지 오웰의 '빅 브라더'와 같이 국민의 사상성향을 조사하고 감시할 수 있게 된 것이다.

이러한 특례조치 때문에 애국법은 공포 후 4년 동안만 발효되는 限時法으로 예정되었지만, 미 법무부 컴퓨터범죄 및 지재권과(Computer Crime and Intellectual Property Section)에서는 테러 위협에 따른 이 법의 존속 필요성을 강조하고 있으며, 시민단체에서는 부시 정권이 이 법의 영속화를 획책하고 있다고 비판하고 있다.[7)]

문제는 미국 정부가 테러와의 전쟁을 내세워 오랜 인권보장의 전통을 무시하고 마구잡이로 일반 시민의 일상생활까지 추적할 수 있게 된 점이다. 또 이것을 가능하게 한 것이 정보기술의 발달에 따른 첨단 전자감시장치이다. 역사는 권력자들이 이러한 권한을 정치적인 목적으로 국민의 자유를 제한하는 방향으로 사용해 왔음을 보여준다. 오늘날 테러 공격의 위협이 상존하고 국가의 주요기반구조가 인터넷으로 연결됨에 따라 어느 나라나 예외 없이 공공의 안전을 위한 정부의 빈틈없는 대응태세가 요구되고 있는 것도 사실이다. 정보화 시대에 있어서 자유(liberty)와 보안(security) 사이에서 균형을 유지하는 것이야말로 국민적 합의를 요하는 국가적 과제라 아니할 수 없다.[8)]

---

7) 이에 관한 주목할 만한 사법부동향은 2002년 5월 해외정보감시법(Foreign Intelligence Surveillance Act 1978)에 의하여 설치된 해외정보감시법원(FISC)이 FBI 등 수사기관과 정보기관의 정보공유를 허용한 감시활동 가이드라인을 프라이버시를 보호하는 헌법정신에 비추어 기각한 사건이다. 이에 법무부가 불복하여 열린 항소심에서 연방고등법원은 2002년 11월 18일 애국법에 의거하여 도청 등 광범위한 감시기술의 사용을 합법적인 것으로 인정하고 수사기관과 정보기관의 정보공유를 허용했다. 국민일보, "美, 反테러 수사권확대 진통", 2002.11.19.

8) 미 법무부는 정부기관 종사자들이 애국법의 내용을 잘 이해할 수 있도록 개정된 내용을 해설하는 홈페이지를 운영하고 있다. <http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm> 여기서 한 걸음 더 나아가 법무부에서는 테러리스트로 의심받는 사람의 DNA 데이터베이스를 만들고, 테러 혐의로 구속된 사람에 대해서는 정보공개청구권을 제한하는 것 등을 골자로 한 "제2의 애국법"(Patriot Act II)을 입안하고 있다고 한다.