EUROPEES PARLEMENT 2009 - 2014

Commissie burgerlijke vrijheden, justitie en binnenlandse zaken

10.9.2010

WERKDOCUMENT 2

over de toekomstige internationale overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de bescherming van persoonsgegevens bij doorgifte en verwerking daarvan met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten, waaronder terrorisme, in het kader van de politiële en justitiële samenwerking.

Commissie burgerlijke vrijheden, justitie en binnenlandse zaken

Rapporteur: Jan Philipp Albrecht

De aanpak van de VS op dit gebied

Grondwettelijk niveau

In de grondwet van de VS wordt niet specifiek verwezen naar een fundamenteel recht op de privésfeer. Toch bestaat de opvatting dat ten minste het eerste, derde, vierde en vijfde amendement het recht op de privésfeer beschermen en ondersteunen. Het eerste amendement beschermt de privésfeer met betrekking tot de vrijheid van anonieme meningsuiting en het recht op geheimhouding van de banden van zijn groep.[1] In het vierde amendement worden de privésfeer en waardigheid beschermd tegen ongerechtvaardigde huiszoekingen door de staat.[2]
In de zaak *Griswold tegen Connecticut*[3] besloot het hooggerechtshof van de VS bovendien dat het individu beschikt over het grondrecht op de privésfeer (privésfeer als "besluitvormingsautonomie").[4]
Met betrekking tot het vierde amendement zijn er problemen ontstaan rond het gebruik door het hooggerechtshof van het criterium "redelijke verwachtingen" ten aanzien van de privésfeer, die in de meeste gevallen grondwettelijke bescherming in de weg lijkt te staan[5], in tegenstelling tot het gebruik van dit criterium bij het Europees Hof voor de mensenrechten.

De Privacy Act

De VS kent geen algemene wet op de privésfeer. In de **Privacy Act van 1974**[6] worden de verzameling, de bijwerking, het gebruik en de verspreiding van persoonsgegevens door agentschappen die tot de uitvoerende macht behoren gereguleerd.

De wet is van toepassing op gegevens die zijn opgeslagen in een 'beheerssysteem' dat *persoonlijk identificeerbare informatie over particulieren* bevat. Federal agencies outside of the executive branch (federal district court, grand jury, probation offices), state and local government agencies and private entities are not subject to the Act. An exception to this rule, however, is the social security number usage restrictions, which do apply to federal, state, and local government agencies.[7]

The Act creates four **procedural and substantive rights** as regards personal data:
- it requires government agencies to show an individual any records kept on him or her;
- it requires agencies to follow certain "fair information practices" when gathering and handling personal data;

---

[1] P. De Hert en R. Bellanova, 'Data Protection from a Transatlantic Perspective: the EU and US Move towards an International Data Protection Agreement?' Onderzoek DG IPOL Beleidsafdeling C Europees Parlement 2008, blz. 13.
[2] Schmerber tegen Californië 384 US 757 (1966)
[3] 318 U.S. 479, (1965)
[4] Voor aanvullend commentaar zie Rouvroy en Poullet, 'The right to informational self-determination and the value of self-development Reassessing the importance of privacy for democracy', blz.20
[5] (nl) blz. 14-15, zie de constructieve aanpak van de zaken Katz en Kyllo, in tegenstelling tot de zaak "Pen Register".
[6] Gecodificeerd onder 5 U.S.C. § 552a (2000). Zie ook het laatste overzicht (2010) van de Privacy Act met gedetailleerde rechtspraak betreffende iedere bepaling van de Act op http://www.justice.gov/opcl/1974privacyact-overview.htm.
[7] (n6) p. 5-9. Also see comments on Social Security Number Usage in (n6) on p.232 to 235.

– it places restrictions on how agencies can share an individual's data with other people and agencies;
– it lets individuals sue the government for violating its provisions.

The Act provides individuals the **right of access and amendment**, but permits an individual to seek access only if his or her record is maintained by the agency within a 'system of records' - i.e., is retrieved by that individual requester's name or personal identifier.[1]

While an agency under the Privacy Act should maintain in its records only the minimum amount of information "relevant and necessary" to accomplish its purposes, there is no condition related to the proportionality of data collections as in Europe. If the information might have an adverse effect upon an individual (by reducing rights, benefits, or privileges), the agency must collect as much data as it practicably can directly from the individual and tell him or her the legal basis, the routine uses to which the data may be put, and the effects that might result from the individual not providing the information.

'Individuals' which have data protection rights under the Privacy Act are defined as citizens of the United States or aliens lawfully admitted for permanent residence, which excludes visitors or aliens.[2] In January 2009, the policy of the Department of Homeland Security Privacy Office has been amended with the effect that 'any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act *regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien*.'[3] Moreover, it is indicated that '[u]nder this policy, DHS components will handle non-U.S. person PII held in mixed systems in accordance with the fair information practices, as set forth in the Privacy Act. *Non-U.S. persons have the right of access to their PII and the right to amend their records, absent an exemption under the Privacy Act;* ***however, this policy does not extend or create a right of judicial review for non-U.S. persons.***'[4] It is an administrative policy which cannot create legally enforceable rights and can be changed anytime. Furthermore, personal data of non-US individuals *not* held in 'mixed-systems' (i.e. systems of records containing personal data on both US and non-US citizens), but in systems of records which only relate to foreigners (such as the US-ESTA) are not protected and not covered by this policy.

Subsection (b) of the Privacy Act limits a government agency's ability to disclose information (**conditions for disclosure**). The agency may disclose such information if it can meet one of the twelve conditions foreseen by the Act, among them disclosure to an agency 'of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity'.[5]

---

[1] (n6) p.92.
[2] In contrast, the Freedom of Information Act (FOIA) does not make such distinction simply referring to 'any person'.
[3] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.
[4] (n10).
[5] This derogation in addition to providing for disclosures to federal law enforcement agencies, it also allows an agency, 'upon receipt of a written request, [to] disclose a record to another agency or unit of State or local government for a civil or criminal law enforcement activity.'

The Privacy Act furthermore provides for ten exemptions, e.g. for agencies that enforce criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and for prosecutors, courts, correctional, probation, pardon, or parole authorities.[1] Nevertheless, such agencies are still bound by the rules on disclosure of subsection (b) and fair information practices.[2]

Agencies have also circumvented information disclosure limitations by exploiting a **"routine use"** exemption.'[3] It is defined as 'the use of a record for a purpose which is compatible with the purpose for which it was collected' and it is required that 'each routine use of the records contained in the system, including the categories of users and the purpose of such use' be published in the Federal Register.[4] This derogation could be problematic when assessed against the principle of purpose limitation and specification.

Other Federal Laws

Other acts relevant in terms of data protection are

- the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. §§ 1801-1811, 1978), as well as the Electronic Communication Privacy Act (18 U.S.C. §§ 2510-2522, 2701-2709, 1986). Both provide standards and procedures for the use of electronic surveillance.
- the Freedom of Information Act (FOIA) (5 U.S.C. § 552, last amended in 2002) provides the possibility, for every person, to access records maintained by US authorities. **FOIA has similar exemptions for the law enforcement purposes as the Privacy Act.**
- the USA-PATRIOT Act (107-56), which, *inter alia,* established "National Security Letters", an administrative subpoena mechanism by which a private entity can be ordered to turn over records and data relating to individuals without probable cause or judicial oversight. NSLs can also include a gag order, preventing the recipient from publicly disclosing that they were even issued.
- the Homeland Security Act (6 U.S.C. § 222, 2002). This Act consolidates and fuses 22 federal agencies into the Department of Homeland Security and *inter alia* provides the grounds for data fusion centers at the state and local level, designed to share information and intelligence.

Supervision

The US has established several structures and mechanisms to conduct oversight, but did not create a central data protection supervisory authority. Among these structures are the Office of Management and Budget (OMB)[5], Government Accountability Office (GAO), each federal

[1] 'Subsection (j)(2)'s threshold requirement is that the system of records be maintained by "an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws."' n (6); p. 213 and onwards for supplementary information on this exemption.
[2] See Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Customs and Border Protection—006 Automated Targeting System of Records http://www.gpo.gov/fdsys/pkg/FR-2010-02-03/pdf/2010-2201.pdf
[3] EPIC The Privacy Act of 1974 at http://epic.org/privacy/1974act/.
[4] (n6) p. 68 onwards.
[5] Subsection (v) of the Privacy Act foresees that the OMB is charged to 'develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing'

department's office of Inspector General, Chief Privacy Officers within federal agencies, a Civil Liberties Protection Officer in the Office of the Director of National Intelligence, the five-member Privacy and Civil Liberties Oversight Board (vacant since 2008[1]), and congressional committees. By means of example, the Inspectors General 'at cabinet level (e.g. DHS, DOJ, Treasury and Defense) are authorised by law to conduct independent investigations, audits, inspections and special reviews of individual actions and programs to detect and deter waste, fraud, abuse and misconduct.' The GAO 'investigates audits and evaluates executive branch agencies and the programs and expenditures of the federal government' and its statue allows it to 'conduct reviews and investigations and issue legal opinions.'[2] It has been posited by some scholars that EU data protection authorities are 'more structurally independent than US privacy agencies'[3] and that the latter generally lack powers to investigate and sanction privacy violations.[4]

Redress

According to the Privacy Act, in order to start a civil action against an agency, the behaviour of the agency must have had an adverse effect on the individual (g)(1)(D). The "adverse effect" of course can be difficult to prove and provides no general hurdle to large-scale data collections and disclosures. It has also been indicated that 'the court should determine that the "agency acted in a manner which was intentional or wilful" (g)(4). Such a complex framework, especially without independent oversight, risks to limit *ex ante* the enforcement of legal redress.'[5] A prosecution enforcing the Privacy Act's criminal penalties provision would properly be filed against an individual. (FOIA) provides limited judicial redress to any individual seeking information about himself. Other Acts such as the Computer Fraud and Abuse Act, the Wire and Electronic Communications Interception and Interception of Oral Communications also provide recourse for an aggrieved individual to file a civil action in US federal court for damages.

An unresolved question and linked to the scope of (non-)application of the Privacy Act, is that non-US citizens or legal residents do not enjoy the right to judicial redress, i.e. to have the lawfulness of the processing of his or her personal data assessed by an independent, judicial authority. In contrast, EU law asserts that every individual in the EU has the right to redress before an impartial and independent tribunal regardless of his or her nationality or place of residence (Article 47 Charter of Fundamental Rights).

Points for debate

Regarding both working documents 1 and 2, at this stage of the process, your Rapporteur wishes to indicate that particular attention should be paid to a number of issues, including:

---

the Act; and to 'provide continuing assistance to and oversight of the implementation' of the Act by agencies. 5 U.S.C. § 552a(v). However, it has no responsibility towards individuals.

[1] Latest information retrieved http://www.washingtonpost.com/wp-dyn/content/article/2010/04/08/AR2010040805470.html.

[2] J Korpf, Networked and Layered: Understanding the US Framework for Protecting Personally Identifiable Information, June 2007 World Data Protection Report, p.5-6.

[3] F Bignami 'The US Privacy Act in Comparative Perspective' available at http://www.europarl.europa.eu/hearings/20070326/libe/bignami_en.pdf.

[4] (n1) p.20.

[5] (n1) p.18.

– the general problem of 'patchworks' of data protection on both sides of the Atlantic,

– the current review of the EU data protection framework, including the integration of data protection law for the private and the public sector,

– the different approach as regards the concept of 'independent oversight',

– the principles of proportionality, data minimization, minimal retention periods, and purpose limitation, including ongoing discussions around profiling and data-mining,[1]

– the definition of the national security sphere,

– the application of data protection rules, including the right to judicial redress, to every individual, regardless of his or her nationality or place of residence.

[1] http://www.coe.int/t/e/legal_affairs/legal_co-operation/steering_committees/cdcj/documents/2010/87th%20CDCJ-BU%20meeting/T-PD-BUR_2009_02rev6_en_Fin%20_2_.pdf