PRIVACY INTERNATIONAL

2006 International Privacy Survey

Ranking by Country

Overview

Each year since 1997, the Electronic Privacy Information Center and Privacy International have undertaken what has now become the most comprehensive survey of global privacy ever published. The *Privacy & Human Rights Report* surveys developments in 70 countries, assessing the state of technology, surveillance and privacy protection.

The most recent report published in 2006 is probably the most comprehensive single volume report published in the human rights field. The report runs to almost 1,200 pages and includes about 6,000 footnotes. More than 200 experts from around the world have provided materials and commentary. The participants range from law students studying privacy to high-level officials charged with safeguarding constitutional freedoms in their countries. Academics, human rights advocates, journalists and researchers provided reports, insight, documents and advice.

This year Privacy International took the decision to use the report as the basis for a ranking assessment of the state of privacy in all EU countries together with eleven benchmark countries. This project was first considered in 1998 but was postponed pending availability of adequate data. We now have the full spectrum of information at our disposal and we hope to publish the rankings on an annual basis.

Funding for the project was provided by the Open Society Institute (OSI) and the Joseph Rowntree Reform Trust.

The 36 countries included in the 2006 survey are all European Union countries, Australia, Canada, the United States, New Zealand, Argentina, Russia, Israel, Thailand, the Philippines, Malaysia, Singapore and China.

The intention behind this project is two-fold. First, we hope to recognize countries in which privacy protection and respect for privacy is nurtured. This is done in the hope that others can learn from their example. Second, we intend to identify countries in

which governments and privacy regulators have failed to create a healthy privacy environment. The aim is not to humiliate the worst ranking nations, but to demonstrate that it is possible to maintain a healthy respect for privacy within a secure and fully functional democracy.

Important note

This study and the accompanying ranking chart measure the extent of surveillance and privacy. They do not intend to comprehensively reflect the state of democracy or the full extent of legal or parliamentary health or dysfunction in these countries (though the two conditions are frequently linked). The aim of this study is to present an assessment of the extent of information disclosure, surveillance, data exploitation and the general state of information privacy.

Summary of key findings

(Please note that "worst ranking" and "lowest ranking" denotes countries that exhibit poor privacy performance and high levels of surveillance.)

- The two worst ranking countries in the survey are Malaysia and China. The highest-ranking countries are Germany and Canada.

- In terms of statutory protections and privacy enforcement, the US is the worst ranking country in the democratic world. In terms of the health of national privacy protection, the US has been ranked between Thailand and Israel.

- The worst ranking EU country is the United Kingdom, which fell into the "black" category along with Russia and Singapore. The black category defines countries demonstrating "endemic surveillance".

- Despite having no comprehensive national privacy law, the United States scored higher than the UK. Thailand and the Philippines also scored higher than the UK.

- Argentina scored higher than 20 of the 25 EU countries.

- Australia ranks higher than Slovenia but lower than Lithuania and Argentina. New Zealand ranks higher than Australia and has an equivalent ranking to the Czech Republic.

About Privacy International

Privacy International (PI) is a human rights organization that was formed in 1990 both as a watchdog on technology and information policy trends and as a monitoring group to track surveillance and privacy invasion by governments and corporations. PI was the first global non-government privacy organization, and has been instrumental in establishing the international privacy movement. It has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, medical privacy, and freedom

of information and expression.

PI's skills and expertise have been used by law reform and human rights organisations in more than fifty countries to assist local issues and by numerous international groups to provide input to global policy issues. PI has worked with more than 200 partner organizations including the American Civil Liberties Union, the Electronic Privacy Information Center, the Irish Council for Civil Liberties and the Association for Progressive Communication. Please see http://www.privacyinternational.org for more information.

Background

In recent years, Parliaments throughout the world have enacted legislation intended to comprehensively increase government's reach into the private life of nearly all citizens and residents. Competing "public interest" claims on the grounds of security, law enforcement, the fight against terrorism and illegal immigration, administrative efficiency and welfare fraud have rendered the fundamental right of privacy fragile and exposed. The extent of surveillance over the lives of many people has now reached an unprecedented level. Conversely, laws that ostensibly protect privacy and freedoms are frequently flawed – riddled with exceptions and exceptions that can allow government a free hand to intrude on private life.

At the same time, technological advances, technology standards, interoperability between information systems and the globalisation of information have placed extraordinary pressure on the few remaining privacy safeguards. The effect of these developments has been to create surveillance societies that nurture hostile environments for privacy.

Governments have created hundreds of key policy initiatives that, combined, may fundamentally destabalize core elements of personal privacy. Among these are proposals for the creation across society of "perfect" identity using fingerprint and iris scanning biometrics, the linkage of public sector computer systems, the development of real-time tracking and monitoring throughout the communications spectrum, the development of real-time geographic vehicle and mobile phone tracking, national DNA databases, the creation of global information sharing agreements and the elimination of anonymity in cyberspace.

The potential for engagement of these developments is currently limited to a marginal response. The problem for civil society – or indeed anyone wishing to challenge surveillance - is not simply the sheer magnitude of the threat, but also its complexity and diversity.

It is important for each country to decide rationally and openly which element of personal privacy should be lost, but it is also important for each country to understand how far down the path of mass surveillance it has travelled. It is for this reason that we have undertaken the rankings project.

The ranking will assess the key areas of surveillance and control, and will identify mechanisms of protection that have failed to operate according to the letter and spirit of the national and international privacy protections. It will concentrate on policy

development issues, inadequacies in the consultation process, legal protections (or lack of them), the impact of surveillance on democratic institutions, changes to the nature of society and the implications for individual freedoms and autonomy.

Methodology

Any comparison of the state of human rights across borders is fraught with difficulty. Even with the mass of data at Privacy International's disposal a large number of variables had to be taken into account. Several criteria originally considered for the rankings were found to be not common to all countries and were thus abandoned. Nevertheless, the existence of a common data protection framework across Europe and other countries provided a stable foundation to proceed with a ranking survey.

After a thorough assessment of the available data we settled on basing the scoring and ranking on thirteen criteria:

- Constitutional protections
- Statutory protection
- Privacy enforcement
- Identity cards & biometrics
- Data sharing provisions
- Visual surveillance
- Communications interception
- Workplace monitoring
- Law enforcement access
- Data retention practices
- Travel & finance surveillance (including trans-border data sharing)
- Global leadership
- Democratic safeguards

Quantitative data was used in most cases. The actual extent, for example, of interception of communications or the conditions and archiving requirements applying to the retention of communications data provided a relatively simple means of comparing the state of those aspects in a variety of countries. A more qualitative assessment was used when comparing such aspects as legal status, identity provisions and global leadership.

A score was awarded for each criterion in each country:

5 = no invasive policy or widespread practice. Leading in best practice
4 = comprehensive efforts, protections and safeguards for privacy
3 = some safeguards, relatively limited practice of surveillance
2 = few safeguards, widespread practice of surveillance
1 = extensive surveillance. Leading in bad practice

The final scores were then distributed over a colour spectrum denoting the overall strength of a country's privacy:

Final Score		
	4.1-5.0	Consistently upholds human rights standards
	3.6-4.0	Significant protections and safeguards
	3.1-3.5	Adequate safeguards against abuse
	2.6-3.0	Some safeguards but weakened protections
	2.1-2.5	Systemic failure to uphold safeguards
	1.6-2.0	Extensive surveillance societies
	1.1-1.5	Endemic surveillance societies

Where adequate information was not available in any particular category a score was not calculated.

The principal research document, *Privacy & Human Rights*, can be viewed and downloaded from http://www.privacyinternational.org/index.shtml?cmd[342][]=c-1-Privacy+and+Human+Rights&als[theme]=Privacy%20and%20Human%20Rights&conds[1][category.....]=Privacy%20and%20Human%20Rights

Categories

1. Constitutional protections

We awarded high scores to countries that have a written constitution with specific reference to privacy. Such circumstances apply to a minority of countries (e.g. Germany). Most countries, for example the United States, have constitutions that have an implied right to privacy, reflected in some judgments.

2. Statutory protection

(see data protection section below)

3. Privacy enforcement

(see data protection section below)

4. Identity cards & biometrics

We assessed the extent and nature of identification practices and proposals in each country, including data sharing between identity and other systems. Any requirement in legislation to present identity was also taken into account, as was any requirement in law to disclose biometric data. The development of conventional elements of enforced compulsory identity schemes was also taken into account. These include *national identity registers, national numbering systems, national identity cards, the* establishment o*f legal obligations* to disclose personal data and the creation of *new crimes and* penalties to enforce compliance with legislation.

5. Data sharing provisions

This section relates to the provision for *administrative convergence* in the private and public sectors and *cross notification requirements* between various administrative functions. The practice is often based on the quest for increased efficiency, but compromises the long-held principle of functional separation under data protection law. The extent of the practice was assessed along with the presence of constitutional and legislative controls.

6. Visual surveillance

This category measured the extent of electronic visual surveillance, in particular closed circuit television cameras. Factors included availability of the technology, safeguards and limitations, requirements by licencing, police and other bodies and use of the technology in private and semi-private locations.

7. Communications interception

Our assessment measured both the extent of interception and the means of oversight and authorization. Most countries have a judicial process for authorization while a small number have an administrative procedure, which we view as less safe. The extent of domestic interception by intelligence agencies was also taken into account.

8. Workplace monitoring

Scoring for this category was based on the nature and extent of workplace surveillance, the availability of safeguards, requirements for monitoring in legislation and employment contracts, the use of employer/employee negotiation and legal remedies.

9. Law enforcement access to data

This category relates the access by law enforcement agencies to the full spectrum of personal information on both criminals and the general population. Aspects include fingerprint and DNA data, criminal intelligence, access to general information systems, access to road and vehicle data, financial data and specific-purpose databases. We considered a range of operational aspects of policing along with capacity for data analysis, data sharing, national integration of data, interoperability and free text searching through systems.

10. Communications data retention

We considered the length of time under law for the retention of data, the legal conditions applying to the retention and the extent of retention.

11. Travel & finance surveillance (including trans-border data sharing)

This category assesses surveillance of the movement of both people and money across the globe. In particular we were interested in the respective role of national governments in pushing for measures to routinely capture, store, process and transmit this data to third parties.

12. Global leadership

This index assesses the extent to which a country has established international leadership either in the promotion of best privacy practice or, conversely, the promotion of the legal, policy or technological means to enable surveillance and avoidance of privacy responsibilities. Whether a country has promoted or resisted poor privacy practice at an international level is a key indicator for this category.

13. Democratic safeguards

We assessed democratic safeguards with regard to the use of such processes as public consultation, parliamentary procedure, openness, accountability and the use of parliamentary oversight bodies. We confined our assessment to aspects related to the above categories rather than democratic safeguards at a general level.

Data Protection enforcement – the crucial element

Each of the EU member states is required under the Data Protection Directive to establish a regulator (sometimes referred to as a Commissioner or Registrar) to ensure that the principles of data protection are upheld. These officials generally have three roles. The first is that of a regulator, responsible for ensuring compliance with law. The second is that of an administrator. The third is that of an advocate and educator, representing the key issues nationally and internationally. Governments to a varying extent rely on the regulator to issue guidance. Citizens are dependent on the regulator to ensure that the letter and the spirit of data protection are upheld.

However, as far back as 1989 Professor David Flaherty, in his landmark study *"Protecting privacy in surveillance societies"* had established that the quality of the regulators varied enormously, often to the point where a regulatory function that in one country might be described as "satisfactory" might be judged in another country to be either non-existent or dysfunctional.

Flaherty identified dozens of factors that influenced the performance of a regulator. He expressed dismay that some jurisdictions suffered from regulation that was patchy, inconsistent or meaningless. Little has changed in the 17 years since Flaherty's study. The difference in style, approach, function, motivation and effectiveness between regulators is as wide as it has ever been. Citizens cannot judge when the regulator fails to adequately uphold data protection.

It is for these and other reasons that we decided to undertake this project. Ineffective data protection law or a timid or compromised regulator can become the lubricant of a surveillance society.

We understand that scoring and ranking regulation is complex. In going about this task we had regard to a number of factors:

Independence. Has the regulator performed a function that can be regarded as genuinely independent? Where independence was not a feature of the post, did the official actively seek to be independent?

Responsiveness. To what extent has the official responded promptly and effectively to issues of concern?

Advocacy. To what extent has the regulator adopted an advocacy role, or has the output been purely administrative or legalistic? Has the regulator made efforts to shift opinion amongst key stakeholder groups?

Forward thinking. To what extent has the regulator worked pro-actively to foreshadow issues rather than merely responding to them?

Outreach.. To what extent has the regulator made efforts to reach affected populations, and to bring disempowered and disadvantaged groups into the regulatory process?

Networking. To what extent has networking been encouraged as a result of action by the regulator? Does the regulator make efforts to involve individuals and organisations other than influential stakeholders?

Case law Where the regulator has such power, have prosecutions been brought by the office to test the application of law? Has the regulator made full use of the powers provided in the relevant legislation?

Education. To what extent has the regulator executed an effective educational function? Have the regulator's decisions and opinions been clear and persuasive in language and relevance?

Transparency. To what extent has the regulator demonstrated best practice in transparency in the decision-making and functions of his Office?

Technical competence. To what extent has the regulator succeeded in deriving knowledge of complex technological aspects at the leading edge both of surveillance and of privacy protection?

With regard to regulation, the benchmarking that we undertook in this report will be useful in several contexts:

- To enable individuals to judge whether the data protection principles are being adequately represented and upheld;
- To enable governments and EU institutions to evaluate the relative performance and output of the national regulators;
- To identify strengths and shortcomings so that efforts can be made to improve performance;

- To create a “best practice competition” amongst regulators who are anxious to improve their performance;

- To assist in the creation of officially recognised performance standards that would harmonise the regulation of DP law throughout the EU;

- To assist civil society in determining the support that each official is likely to provide with respect to data protection issues.