Freedom of information versus privacy: Friends or foes?

S. Gutwith et al. (eds.), *Reinventing Data Protection?,* Springer Science+Business Media B.V., 2009, pp. 293–316, DOI 10.1007/978-1-4020-9498-9

The final publication is available at
http://www.springer.com/law/international/book/978-1-4020-9497-2

Freedom of Information versus Privacy: Friends or Foes?

Ivan Szekely

1. On the Relationship between the Two Concepts

Behind the anomalies currently besetting the notion of privacy – anomalies that arise from different cultural, political and social milieus both at the group and at the individual level – there lies a common conceptual element: individuals and small communities carry an increasing weight vis-à-vis the external world. This conceptual element is reflected in the various manifestations of privacy, whether as a social phenomenon, or as a value, or as a right, written or unwritten, or as a political goal, or even as a marketable commodity.

The notion of freedom of information (FOI) shows similar anomalies, whether we look at it in a historical context or study it from a geographical, cultural or political perspective; and, these, too, share a common element, which is the pivotal role assigned to individuals in their dealings with one of the fundamental actors of the external world: the modern state.

The view whereby these two concepts clash and mutually limit each other has been gaining popularity.[1] In other words – according to this view –, a legal system or a social establishment must decide whether it prefers freedom of information (together with the associated concepts of transparency and accountability) at the expense of respecting and protecting people's right to privacy, or the other way around. In black and white, one should envisage it as a zero-sum game, in which we must take away the same amount from the implementation of one concept that we add to the implementation of the other, and it is entirely up to us where we actually draw the line.

This approach is based on a fundamentally flawed interpretation. If we were to ask what were the ultimate goals of the two 'competing' concepts from the viewpoint of the individual, then we would come to the conclusion that it was the same one: both are meant to protect the individual citizen from excessive information power.

[1] In some cases this view is based on misunderstanding of at least one element of this relationship: even a 'Comprehensive Information Assurance Dictionary' can contain expressions relating to data protection in a misleading sense (Shou et al. 2002), or a European law firm in its statement seems to confuse data protection legislation and secrecy legislation (Louis 200?); similarly, the notions of confidentiality, data protection and freedom of information seem to be muddled in the health sector (see for example Theale Medical Centre 2007). In other cases the approach is correct but the analyses emphasize the conflict between the two areas (e.g. Pitt-Payne 2007, Singleton 2002).

1.1 The Citizen and the State

Our current notions of privacy and FOI are strongly related to the power relations between state and the citizen, although none of them can entirely be reduced to that. In the case of privacy, it is evident that the boundaries cannot be limited to the state, as we also have the business world, the civil organizations and even other individuals to consider. The freedom of information – in short, the individuals' freedom and fundamental right to accessing public information – is, in theory, only meaningful vis-à-vis the public sector, but in reality the borderlines are beginning to blur: in the practice of modern state administration, several of the state's functions are outsourced to the business, and even the civil, sector.[2]

In the field of information, any relationship, even a momentary one, has a stronger and a weaker side. The stronger party always has more information about this relationship; typically, the weaker parties cannot even be sure what it is exactly that the stronger side knows about them. It is sufficient to remember only the day-to-day power relations between state and citizen or service provider and customer.

If we study the changes from the abstract viewpoint of power relations, rather than from a purely legal aspect, then we shall find that the application of modern information technology has greatly altered the earlier balance: the stronger side has mostly become even more powerful, the weaker even more vulnerable. One branch of the arising problems originates from the changes in the information boundaries of the private sphere, i.e. from the concentration of information power *as a factor in monitoring and influencing the individual,* while the other main branch stems from the changes in the information status of the individuals, which determines their participation in society, i.e. from the concentration of information power *as a monopoly on handling public information.*

The guaranteeing of privacy, most notably of information privacy, serves – in tandem with the European system of laws and regulations, as well as with data protection and other available means and methods to carry out data handling – to counter-balance the former of these two influences. The freedom of information helps dampening the latter. What they share in common is that they constitute an essential element in the information autonomy of the individual. On the one hand, this is assuming that data protection functions as an active right of informational self-determination, going well beyond its traditional, protective legal character; in other words, the individual should be able to decide when, how and to what extent the information on his or her person can be accessed by others. On the other hand, a similarly fundamental element of information autonomy is the ability of the individuals to access information in the public sphere – even to the extent that he or she should be able to decide, within the possibilities available, what information to receive and what to reject – in other words, the option of rejecting unwelcome information (propaganda, marketing) should be left open. It is evident that the state and its citizens (analogously, of the business sphere and the customers) should have significantly different information utopias, and in its purest forms, neither can be implemented. But the key factor in both scenarios is the extent to which each side, i.e. the stronger and the weaker, has the ability to access information about the other.

[2] See: Alasdair S. Roberts: Structural pluralism and the right to information (Roberts 2001)

1.2 Cultural and political dichotomies

From the above it follows that, rather than being diametrical opposites, the concepts of information privacy and freedom of information in fact complement each other. The ideals behind them – the transparent and accountable State and the autonomous, self-determining citizen – are interdependent sister concepts. Although they were undeniably produced by the Western cultural hemisphere in modern history, these sister concepts in some sense constitute outstanding achievements in social and legal developments. From a Western perspective it may appear that these two elements of the twin concepts are fundamentally alien to the cultural East. Since the notion of *individuum* does not have the same importance in the East as it does in the West, individual autonomy in the field of information is not a fundamental demand of the citizens living in Eastern societies – and vice versa: the eastern citizens do not want to hold their leaders, sovereigns and state bureaucracy to account. While such a sweeping generalization is not entirely unfounded, it is not entirely true, either. On the basis of my brief experience in Korea, in cultures rooted in Confucian traditions the respect of individuals also includes the respect of the 'information self'. From the analysis of Western observers there emerges a tradition, which I personally would describe as 'virtual privacy': if the physical environment does not permit the implementation of privacy, then the participants will achieve it by the wilful elimination of mutual perception.[3] The respect of the individual is also reflected by the use of modern information and communication technologies in the countries of the cultural East.[4]

The dichotomy of dictatorial regimes and democratic establishments offers a different comparison (although here, too, we rarely see the extremes appear in their purest forms), which is manifested in a grotesque symmetry. While the transparent, accountable State and the autonomous, self-determining citizen are the ideals of the democratic establishments, those of the dictatorial regimes are the autonomous, self-determining State and the transparent, accountable citizen. The elderly and the middle-age generations living in Europe's 'new democracies' had ample opportunity to experience the difference between the two.

2. Conflicting areas

If we accept that in a democratic society privacy and freedom of information are two concepts that complement each other, instead of competing with each other, than there is no need to 'balance' the two concepts in general – and the present paper could end here. However, although the two concepts do not clash head on, they have certain interfaces or conflict zones. While the existence of these zones does not question the complementary nature of the two concepts, marking the borderline between the implementation of the two is not always easy in practice.

[3] For more details, see Crane [1967] 1999, especially p. 62, on the encounter of the master and his disciple.

[4] This is the topic of a recent study by a Hungarian student following a field trip in Japan: Vincze, B., Protection of privacy in using modern information technologies in Japan.

Of these conflict zones, we would like to focus on two in particular. We can outline them with the help of the following questions: Firstly, does a public servant have a private life? Secondly, does the information about collaborators of former (dictatorial) regimes constitute 'data of public interest'?

2.1 Public service and private life

In everyday usage, public service refers to a form of employment, which in theory implies a dedication to serving the public, and in practice means a job with the associated duties in some government institution. The democratic state – we are still speaking theoretically – executes the will of the people through representatives elected by the public, and these representatives entrust various organizations with the job of carrying out the 'will of the people'. These organizations are financed by the taxpayers' money to carry out a public mandate – and so the public has every moral right to monitor their activities and to hold the people in charge to account. In the majority of the democratic states this moral right has been transformed into codified rights and freedoms, or in the case of their most advanced form, a universal right of everyone to access public information or 'data of public interest': the freedom of information.

If we take the data belonging to the domain of information privacy – i.e. personal data – to be a well defined set, then we shall be able to place right next to it the set of data of public interest, which includes the data that constitute the domain of the freedom of information (Fig. 1). Actually, by doing that we have also defined the most fundamental categories of information about the state and the citizen.

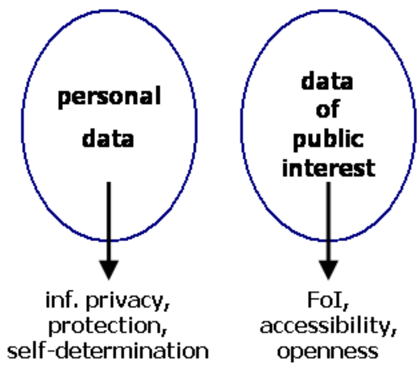

Fig. 1

The dischargers of public service are, naturally, not merely abstract legal entities and institutions, but real people who work in these institutions – people who are entitled to the rights to privacy, including the right to information privacy in particular. To what category does their personal data belong? Or to put it differently: Do public servants need to surrender the rights that they are otherwise entitled to as private persons or as individuals? We can approach this problem from two directions. On the one hand, in modern societies individuals fill various positions in various communities and, in accordance with that, they perform various roles, including the written and unwritten rights and duties that are associated with those roles.[5] Public service is one of these distinguished roles, which may be associated with different (written and unwritten) rights and obligations. On the other hand, we could say that a public servant is quite simply not a 'private person', but a representative of the people and at the same time a servant of the state. And in that capacity, he is subjected to rules and regulations that are different from the ones that apply to private individuals in general.

Once we have adopted the latter approach, our problem apparently becomes a very simple one: in all activities one carries out in his or her capacity as a public servant, he or she cannot be regarded as a private person and, therefore, all the information that are produced in connection with that activity are 'data of public interest', to be handled according to the principles and rules associated with FOI. So does it follow from this that the personal data of public servants are actually not personal data, they belong to the domain of data of public interest?

It should be pointed out however that a public servant also has a private life, and the two roles belong to the same individual: the information generated in the course of performing the two different roles can be associated with the same person. Therefore, the two sets will partially overlap and an intersection will be created (Fig. 2).

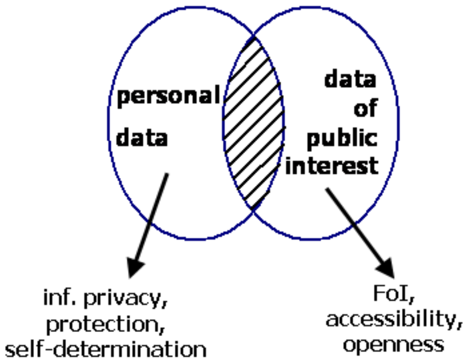

Fig. 2

Here, too, a seemingly simple solution presents itself: The data protection rules, which have been introduced in order to guarantee information privacy, should not apply to those data, which are created in connection with public service activities. So does that mean that these data do not constitute personal data? No, it doesn't mean that: according to European legal philosophy and dogma, personal data do not lose their personal character on account of their public service environment. These are personal data, to which the principles and practical rules of data protection and informational self-determination do not apply, or do not apply entirely. If the main principles regarding public service are transparency and

[5] The preservation of this multi-role character constitutes one of the most important questions in the protection of privacy in the era of surveillance society and integrated information systems.

accountability, then the main principles regarding these personal data should be openness and public access (Fig. 3).[6]

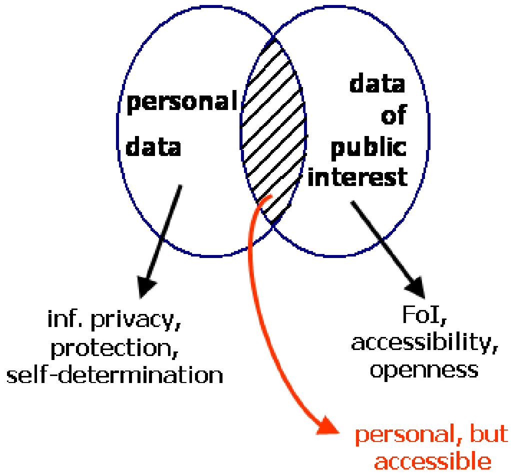

Fig. 3

However, drawing the borderline is not always easy. On the one hand, in numerous countries the information rights associated with these two domains are regulated in separate laws and bylaws, and sometimes they do not fully cover the overlaps or intersections. On the other hand, the day-to-day practice of public service often throws up problems that do not lend themselves to trivial solutions on principles, and they are not covered in the relevant legal articles.

Where do the boundaries of the overlap lie? Or to rephrase the question: Where do the boundaries of a public servant's private life lie? I personally know public servants who take great care to make sure that their private lives are well separated from their professional capacity. By the same token, I also know public servants who take their work home with them, allowing it to become part of their private lives, thanks to the blessings – or curses – of modern information and communication technologies. And I also know public servants, whom people on the street recognize, thanks to their high-ranking status or public appearances, with journalists stopping them for an interview while shopping. However, I know of no such laws or legislations, which adequately regulate either these situations or the handling of personal data under these circumstances. I can only confirm the existence of a linear relationship between the position of a public servant and the size of the overlap: the higher position a public servant has, the greater is the overlap, and also, by implication, the narrower is the extent of his or her private life (Fig. 4).

[6] In Hungary, where data protection and freedom of information are regulated by a joint law, certain public servants tried to abuse their data protection rights immediately after the enactment of the law (in the early 1990s): they refused to release documents to applicants on the ground that these documents bore their official signature – their personal data.

How wide?

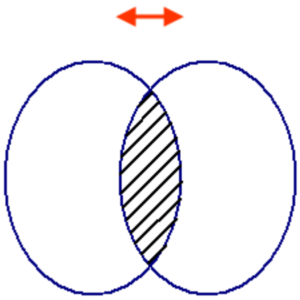

Fig. 4

In an authoritarian society or social milieu even the journalists tend to subscribe to the view that the private life of a prime minister is sacred, because he is a very important person, while the private life of his secretary is less so, because she fills a less important position. In reality, quite the opposite is true. The private life of a secretary is more important, because her role and lifestyle more closely approximates that of a private individual. And as for all the things that 'important persons' can do to secure the physical boundaries of their private life (surrounding their residences with stone walls, hedges or security guards), it is important to remember that they cannot do the same regarding the information about their private life (notably: their personal data), at least not in principle.

What about the time scale of the overlap's pertinence? The most obvious frame of reference in this could be the duration of the working hours. According to this, all the data generated in the life of a public servant on workdays before 8 am and after 5 pm, and all day on weekends, are private information and should be beyond public scrutiny. However, even after deducting the hours spent working overtime or working at home, there exist a much longer cycle, too: the duration of a public service career. Can someone's status as a public servant legitimate public scrutiny of personal data relating to an earlier period? The accountability of a minister is more far-reaching than that of a clerk, but what happens when a clerk becomes a minister at a later stage? Can he be called to account about events that took place before his appointment as a minister? The same dilemma presents itself in relation to a minister who has been retired for years, but the tabloid press sustains an interest in him on account of his former position (Fig. 5).

How long?

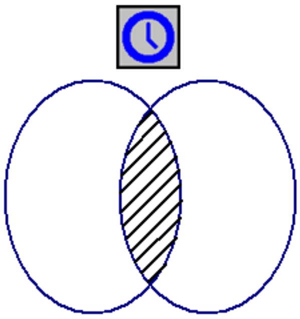

Fig. 5

And finally: Is it possible at all to separate a person's identity as a private individual from his/her capacity as a public servant during working hours while doing public service work? Like every other employee, a public servant takes private telephone calls, writes private e-mails, and conducts private affairs during work, not mentioning occasional visits to a café or to the restroom. It is quite obvious that his/her personal data related to these activities should not concern the public – except for the cases, when the taxpayers' money is being squandered for private purposes, or when one is found in gross neglect of one duties, or when one abuses one's official power (Fig. 6).

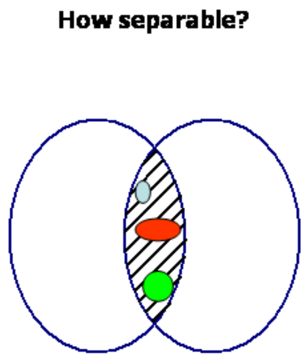

Fig. 6

The key element in all the numerous questions raised above is *public function*. We can declare that the main clause of the freedom of information applies to all the personal data, which are related to the conduction of public service – irrespective of the actual location and time, i.e. whether it is done during or outside working hours, at the workplace or at home; furthermore, it is clear that the higher is the position the public servant in question occupies, the broader is the range of personal data that should be made open to public scrutiny.[7] On the other hand, the possible range of private data can vary according to the social, political and cultural traditions and tastes, as manifested, for example, in the differences between the public scrutiny given to the health condition and sexual life of a US President or a presidential candidate on the one hand, and that of the heads of states in Europe, not to mention Eastern Europe, on the other.

2.2 Lustration

This expression gained currency in the new European democracies during the years immediately after the political transition. It was introduced in reference to the process of 'cleansing': the attempt to screen out persons who had participated in the activities of the

[7] The logic behind this reasoning can appropriately be applied to employees working in the private sector, also, but in that case it is not the freedom of information that limits the private life of the employees, but the employers' thirst for information, which leads to the tapping of telephone conservations, the monitoring of private e-mails, and occasionally even the use of polygraphs. However, here, too, the activities carried out on behalf, or in the name, of the company can be separated from private life, the representation of the company's interests from activities conducted as private individuals.

Communist state security forces, either as paid informers or as enlisted personnel.[8] It is not the aim of the present paper to discuss the various motives, personal interests and moral justifications of people who took part in those activities, either as official members of the organization or as writers or readers of surveillance files, but the lustration laws apply to all of them equally. The actual model chosen to find a solution for the problem varied from country to country.

The screening process has three main objectives: the first one is lustration, which aims at ridding the public life of the persons who had carried out activities irreconcilable with the democratic legal system (this is the penal element); the second is the unveiling of the activities of the secret police under the one-party state system (this is the element of information restitution); and the third is the provision of access to personal files for the individuals concerned (this is the element of informational self-determination). The three objectives received different emphasis in the legislation and practice of the various countries: in some countries, the main objective was to unmask the former informers and oust them from positions of influence; other countries focused on the retroactive implementation of informational self-determination; and the rest assigned priority to unveiling the system of spying.

One of the sanctions introduced had a bearing on information rights: the clandestine activities of the perpetrators were published. This elicits the following question: Should, therefore, the relevant activities of unpaid collaborators be treated as 'data of public interest'? Is the disclosing of these data a question of freedom of information at all? In our view, public access to information regarding the collaborators' activities as a *social phenomenon* (and also the operation of the secret police) belongs to the realm of FOI. By contrast, information about the activities of individual collaborators already belong to the overlap: to the domain of *personal* data, however, governed by the main principles of transparency.[9] The grey area this time is outlined by the boundary between the mandatory publication of personal data and the limitations on the publication of data of public interest (for example, state secrets).

In a paradoxical manner, in weighing the options about the publication of personal data, here, too, the key element is the public function. An officially employed secret policeman naturally filled a public function – he was a 'public servant' in the broader sense of the word – even though the public was not able to learn about his work; according to our current notions, this is what justifies the publication of his personal data. But the private citizen who wrote the reports voluntarily was not employed by these organizations, and quite often

[8] I would like to point out that in the controversial and murky waters of retroactive justice-making the only reason why retroactive sanctioning can legally be justified is that the activities of the previous political regime's secret police had violated the constitutional requirements of even *that* establishment.
[9] This is why, in my opinion, the Constitutional Court's resolution 60/1994 (XII.24.) caused severe damage in the conceptual framework of Hungarian information rights, when it declared that, according to the Constitution, the information concerning the earlier activities of people presently active in public service or politics, activities that are irreconcilable with the democratic legal system, were '*data of public interest*'. It could have declared that these were personal data, the disclosure of which lied in the public's interest; alternatively, it could have said that these were personal data, which would need to be published by force of law; or that the decision to give public access to these data did not lie with the person concerned. The actual wording of the resolution, however, implicitly stripped these data of their personal nature.

received no salary or any other rewards for his acts. But through his act he rendered a form of public service – again, in a broader sense and with an ironic overtone – and so (besides the social justice) this could justify the publication of his personal data.

3. Evolution or Erosion?

Viewing it from a historical perspective – and leaving aside the wartime or dictatorial excesses – freedom of information and information privacy seem to be moving in the opposite directions: in fully fledged democracies, more and more people are being aided by more and more rights and more and more technological means to access public information; parallel with that, they more and more seem to be losing the capacity to dispose over their personal data.

In the history of rights to public information, the first agents to gain the right to disseminate information were the intermediaries between the source of information and the end users. Such intermediaries were the representatives and the media. At the next stage, the intermediaries, in addition to passing on information, also won the right to demand information. In other words, people in possession of a press card or a delegate's card received privileges in accessing information. Finally, the end users themselves gained the right to ask for and to receive answers directly. This is where we are at the moment in the case of the majority of the most advanced democracies, at least in theory. Therefore, the legal development of access to public information can be presented by an evolutionary model.

By contrast, the traditional boundaries of private life have continued to erode, precisely on account of the changes in information relations, the overall result being that, when seen from the viewpoint of the earlier value systems, the spread of new information technologies has produced negative rearrangements at a social level. First the technology of *acquiring* information about individuals went through revolutionary changes (telephony, photography);[10] next it was the element of information *processing* that led to fundamental changes (computerized data processing);[11] and finally the two element mixed irreversibly, creating a new dimension in the handling of personal information (let us simply call it the Internet world).[12] Naturally, the development of privacy and data protection legislation reveals positive, evolutionary tendencies, while the practical enforceability of the rights thus codified shows clear signs of an erosion.

The processes outlined above mainly characterize the most developed countries, which are often described as traditional democracies. In the case of the new democracies, the dynamics of both the evolution and the erosion is different. While before the Second World War, the countries now referred to as the 'new European democracies' were *not yet able* to reach that stage of democratic legal development, which could have organically allowed the development of a full catalogue of human rights, along with the modern system of new

[10] The environment that led to the initial conceptualization of privacy by Warren and Brandeis.
[11] The environment that led to the promulgation of classical data protection laws.
[12] The environment that led to the need of 'reinventing data protection'.

information rights (including the legal and institutional guarantees of ensuring privacy and FOI), in the decades that followed it[13] they were *no longer able* to do the same.

It is quite apparent in the case of these countries that the euphoria of the democratic transition engendered an ardent demand to curb the state's omnipotence in information power. This demand concerned the creation of the state's transparency and accountability (with a special emphasis on the disclosure of, and access to, documents of recent history), as well as the restraint of its power to monitor people's private life. Despite the adverse effects of society's over-politicization, human rights in general became more important throughout this period, and this created a favourable environment both for the legal codification of information privacy and FOI and for the creation of the institutional system monitoring their implementation. But the euphoria subsided after a few years, the new or reformed legal system was put in place; the public could witness the emergence of new or restored government structures; and a new generation grew up, for whom the new values of capitalism, such as the belated original accumulation of capital, the enjoyment of material possessions, career and political power, enjoyed priority over respect for human rights, including information rights. In this regard, the countries, which took advantage of the historic opportunity and rode the tidal wave of democratic transition to install the legal and institutional guarantees for the implementation of information rights, can count themselves lucky. In summary, therefore, the development of information privacy and FOI in the new democracies has shared a common dynamics, characterized by rapid development first, and followed by gradual erosion.

And if we were asked to identify the source of influences *simultaneously* working towards development and erosion in the new democracies, then we would have to name the advanced democracies of the West, which had exerted a paradoxical influence on them. The new international relations, the obligations and the commitments together had a controversial effect on the implementation of the information rights in the countries undergoing democratic transition. On the one hand, the international community expects the new democracies to provide legal guarantees for the realization of individual rights and freedoms, including the free access to public information and the protection of information privacy. On the other hand, their newly conferred NATO membership, the urgency to join the Schengen zone – along with the additional tasks that would entail – as well as the cooperation with Europol and other international investigative agencies, not to mention the economic and political ties with the United States, all tend to put pressure on the above mentioned countries to limit self-determination over personal data, to extend the laws on classified information, and to be cooperative in anti-terrorism campaigns, all of which assumes the curbing of the recently granted information rights.

3.1 Further similarities and differences

If we consider the phylogenesis and the ontogenesis of data protection and freedom of information legislation (i.e. the historical processes of the creation of the two codified law and their respective careers in the various countries), it will immediately be quite clear that

[13] In the case of the republics of the former Soviet Union, during the period between the two World Wars.

the group of newcomers, which only recently joined the community of countries with legal guarantees of data protection and FOI, have gone through more or less the same stages as the pioneers had. Moreover, the steps taken are remarkably similar in the two areas under scrutiny.

The first step in the area of privacy protection (usually prompted by some external actuality) is the start of scholarly research. Ahead of their time, a few advocates, specialists and scholars issued warnings, which was usually followed by the various national governments' decision to set up committees, made up by serious scholars and specialists, with a mandate to investigate the consequences of computerization on people's private lives.[14] The 'late-coming countries' usually skipped this stage in their national development, although even in the case of the new democracies those few scholars and specialists, who were familiar with the topic and had contact with the specialist of the developed democracies, were helping the work of the drafting committees behind the scenes.

In the area of FOI, the phase of scholarly committees was skipped, and the development began after the Second World War with the appearance of advocacy and lobby groups. [15] The formation of informal coalitions determined to exert pressure on legislation soon followed both in the area of FOI and that of information privacy and DP alike.[16] Their members typically included advocates, civil organizations, sympathetic MPs, a considerable faction of the press, and the prominent representatives of the legal and the informatics professions; the opponents were made up by government officials and representatives of the counter-interested business sector. Subsequent to this phase, in each country where the work of drafting the bills took place in a calm social and political milieu, the debates remained within the bounds of professional discussions, while on each occasion that they were accompanied by social tensions and political quarrels they assumed the character of a party political campaign: one of the political sides stepped forward as a resolute champion of information rights.[17]

The actual passage of the law has come to constitute some kind of a watershed in the development of both information privacy and FOI, as not every one of the countries that set

[14] A classic example is the British government's decision to set up the Younger Committee, which incorporated in its 1972 Report the results of a highly advanced sociological survey, as well as a study of the evolution of the notion of privacy. A similar committee was founded in France, which published its findings – the Tricot Report – in 1975; then back in Great Britain the Lindop Committee was set up, which published the results of its research in 1978; the task of these committees was, among others, to lay the grounds for the legislative work. In the US, the House of Representatives Special Subcommittee on Invasion of Privacy held hearings as early as 1965, while the Secretary's Advisory Committee on Automated Data Systems, commissioned by the Department of Health, Education and Welfare submitted its report entitled "Records, Computers, and the Rights of Citizens" in 1973, providing ammunition to the birth of the USA Privacy Act.

[15] Here is a cursory list: one such group in the 1960s was the Ralph Nader Center for Study of Responsible Law in the United States; another one was Campaign for Freedom of Information, founded in 1984 and still active in Great Britain; National Campaign for People's Right to Information (NCPRI), a national platform set up in India in 1996, which led to the birth of the Right to Information Act in the various member states first, and eventually nationwide in 2005.

[16] Among the coalitions, we can find some formal organizations, also, such as the earlier mentioned NCPRI in India, or Citizen's Initiative in Slovakia, with the latter becoming a coalition of 122 civil organizations and launching a campaign that led to the passage of an information access law in 2000.

[17] As David Flaherty, former Information Commissioner of British Columbia, Canada, once noted ironically: politicians simply love the idea of freedom of information – *before* and *after* they are in power.

themselves the task to guarantee the information rights actually reach this stage: in a legal sense, this implies the establishment of sectoral laws and regulations, as well as the creation of independent, monitoring institutions. Several countries have got stuck at the level of a 'single act', which makes the system extremely vulnerable, even where the fundamental principles have been incorporated in the constitution. Parliaments can quite simply modify or limit a single act, and in the case when the constitutional guarantee is lacking, the incumbent administration can easily introduce modifications. (Sweden offers an extremely positive example concerning the constitutional guarantees of freedom of information: its FOI Act actually forms part of the country's Constitution.[18]) Typically, the countries that imported the idea and the legal guarantees of data protection and freedom of information relatively late – some new European democracies included – passed only one law, either in one or both of the two areas. In the implementation of the law, this also means that the administrators regard it as a one-off and exotic piece of legislation, which should be used only in special cases; in other respects, numerous questions regarding its application, minor points and harmonization with other legislations are left open. By contrast, in countries, which decided to put in place an entire system of codified information rights and freedoms, a brand new legal branch was created, which entwined the complete legal system with a logic that was slightly different from that of the traditional branches, such as the areas of public and private law.[19]

Similarly, not every country reaches the stage of setting up independent institutions for monitoring the implementation of the law. But even in countries that have reached this stage, the efficiency and the public perception of these institutions can occasionally display wide variations. In countries, where either the institution as a whole, or its current leader, or perhaps just the occasional reactions and statements issued by the leader, draw public criticism (not from the counter-interested parties, whose power positions, political or business interests are threatened by the implementation of data protection or FOI laws, but from civil society or the profession), we are likely to encounter the stirrings of professional or civil disapprobation, which could lead to the intervention by radical civil organizations. Actually, the latter phenomenon is a rather paradoxical one, since these are essentially two manifestations of the same type of 'legal protection' organizations, which from time to time undertake the same tasks. For example, the Hungarian Commissioner's statements concerning CCTV issues provoked some civil organizations into nominating him for one of the prizes of the Big Brother Awards,[20] the Audience Prize, which he received in 2004.[21]

[18] The Swedish Constitution consists of four fundamental laws, one of them is the so-called "Freedom of the Press Act", which in fact is a FOI law.
[19] For example, at present Hungary has nearly 1000 acts and regulations that contain provisions on data protection and the processing of personal data.
[20] The negative prize invented by Privacy International that has been adopted in several countries.
[21] This case aroused animated debate among NGOs and activists. Is it legitimate for civilian advocates to resort to such measures to censor the official guardian of informational rights? And what does this criticism really reflect? The opinion of society on the whole, or the views of a handful of hard-line activists? Of course, no one should reasonably expect a civilian organization to dedicate itself to all-out impartiality or to consistently choose the golden mean. The voice of an NGO is generally a radical voice, crying out from a marginal, minority position against an injury perceived in a disturbed equilibrium – this is in fact the essence of its social mission. In the case at hand, however, the minority was certainly not an easily dwarfed one, for the panel consisted of renowned professionals and public figures. They may not have acted as the mouthpiece of some 'official' consensus, but each of them certainly provided an authentic, one-person representation of the opinion formed by various social and professional groups.

Although data protection and freedom of information have run a similar course in history, the pace of development has been different at the international level. Thanks to Sweden, and also to the influence Sweden wielded in the Nordic countries,[22] FOI had an early start; however, in terms of the number of countries that took over the idea and codified their own FOI Acts, the development was slow. Then, beginning with the early 1990s, it picked up some speed, and eventually finished very strongly, thanks to the new democracies, which launched a wave of legislation after the turn of the millennium.[23] The codification of information privacy, understood in the modern sense, started later;[24] it had a few bumper years in terms of the number of countries joining, but at the moment it seems to be yielding ground to other legislative priorities. There are probably more FOI Acts around globally (approximately 70), than there are privacy or data protection acts (about 55), although their enumeration is rather difficult because of discrepancies, of both form and content. (These estimates are based on the annual global reports of EPIC[25] and Privacy International,[26] as well as on the registries of international organizations.) At the same time, there are more Privacy/Data Protection Commissioners (approximately 45), than Information Commissioners (approximately 22); their number can be estimated by the attendance figures of their annual conferences.

3.2 Common solutions

With all their similarities and dissimilarities, information privacy and FOI are mutually interrelated and mutually interdependent concepts. Among the formulas designed to handle simultaneously the issues that have emerged in connection with marking the boundaries of these two areas and defining their detailed regulation, there exist a few tested models, which are internationally recognized as successful.

One such model is the joint, or at least interrelated, legislation of the two areas. In Canada's Provinces and Territories,[27] legislation passed combined acts, and these laws have proven their viability for many years now. The main advantage of regulating these areas in a combined act is that in this way the boundaries of the legal conflicts between the two information rights are clearly drawn, thus precluding the possibility of playing off one against the other: in other words, it makes it impossible to justify the curbing of one right in the name of the other. In the case of the new European democracies, Hungary chose the Canadian model in drafting its own combined data protection and freedom of information (DP&FOI) act. In addition to the necessity to harmonize the two areas to be regulated,

[22] Finland, being a part of the Kingdom of Sweden, first introduced the Swedish FOI Act; it enacted its own law in 1951.
[23] See Alasdair Roberts' impressive chart (Roberts 2006, p. 16.)
[24] The earliest piece of modern data protection legislation was enacted in the German province of Hessen in 1969; it was followed by Sweden's Data Act of 1973 and the US Privacy Act passed in 1974.
[25] Privacy and Human Rights, published by the Electronic Privacy Information Center
[26] Freedom of Information Around the World.
[27] With the exception of New Brunswick, similar joint laws – largely promulgated in the 1990s – are applied in all the Provinces and Territories. In addition to these pieces of legislation, which originally were only applied to the public sector, many of the Territories introduced new, separate Privacy Acts, which already reflected the concept of the new, federal Privacy Act, and had their effects also extended to the data controllers in the private sector.

Hungary was also motivated by certain political considerations in its decision: the experts drafting the legislation did not want to run the risk of the Parliament's approving the bill in one of the areas and rejecting it in the other, in an area that concerned constitutional rights and, therefore, required a two-third majority – in other words, the opposition's cooperation.

The other way to resolve the problem is to assign the task of independent supervision for both areas either to the same person or body. Those countries and sub-national territories, which opted for the combined act, appointed a joint, independent agency for the supervision of both areas. However, the practice of setting up joint supervisory agencies has been spreading even in among countries, which legally regulate the framework and guarantees of information privacy and FOI in separate laws – mainly as a result of the positive examples set by similar institutions functioning elsewhere. Naturally, having a joint supervisory body is more cost-effective, as only one office needs to be set up and run for the Commissioner or the Ombudsman, instead of two, but this is not the only advantage. In those instances, when the Commissioner's or the Ombudsman's statement, recommendation or verdict is sought in connection with issues concerning the grey areas of the overlap, there are clear advantages in both the practical realization of uniform interpretation and the quasi-caselaw consequence in both areas, not to mention the advantages that lie in avoiding the situation, where the two independent supervisors of the two areas come to diametrically opposite conclusions. To demonstrate the reciprocal effects that old and new democracies can occasionally exert on each other, it is worth mentioning the example of Germany and Hungary: in establishing its new system of information rights, Hungary borrowed the German model based on informational self-determination; as for the advantages of joint supervisory agencies, the various federal states in Germany had been encouraged by the Hungarian experiences before setting up their own institutions.[28]

There are further joint possibilities in education: not just in regular school education, but also in the formal and informal education of citizens, data controllers, public officials, journalists and IT experts. In today's strongly specialized world, these actors have a tendency to view these two areas as isolated, depending on which one of the two rights' realization or limitation happens to be in their interest at that moment. Developing an understanding of the joint system of information rights helps these actors in acquiring, or at least learning, the norms of lawful and ethical behaviour, even when their momentary interests seem to dictate otherwise.

It is interesting to note that a certain convergence seems to exist among those civil organizations and movements, which were originally active in one of these two areas. This convergence can be discovered in two areas: one is the cooperation among organizations engaged in the propagation of information privacy and FOI, as manifested both in the mutual support they lend to each other's actions and campaigns and in the establishment of coalitions; the other is the civil organizations' tendency to broaden the scope of their interests, mutually extending their activities to the other sphere. An example of the latter is

[28] The hearing of the Hungarian DP&FOI Commissioner in the Brandenburg legislation in December 1997 played a crucial part both in the creation of Brandenburg's FOI legislation and in the establishment of the institution of joint parliamentary commissioner; Brandenburg's example was soon followed by Berlin and Schleswig-Holstein (for more details, see Dix 2001).

EPIC, which has, in the course of the last few years, gradually extended its interest to other areas of information rights, such as free speech, open government and freedom of information. The situation is similar with Privacy International (partly due to personal factors, but also thanks to the expansion of structural concepts), which has been active also in freedom of expression and FOI.[29] Another relevant example is the Access to Information Program (AIP) in Bulgaria, which deserved a fair share of the credits in connection with the passage of the Bulgarian access law, the education of the public officials and the monitoring of the FOI-related cases,[30] and in the last few years it also turned its attention to the protection of personal data.

4. Neighbouring areas

From the viewpoint of privacy, the requirements of self-determination over, and protection of, personal data can, in certain cases, be curtailed not only by FOI, but also by some of its neighbouring areas. By way of a brief demonstration, we mention two such areas in the following.

4.1 Freedom of information and freedom of expression

According to a well-known concept, freedom of information and freedom of opinion and expression both belong to the common family of 'communication rights': each of them traces its origin to the same ancestry in communication law. From the viewpoint of this concept the realization of this fundamental communication right is limited by information privacy. There are, however, other comprehensive theories, which place privacy itself among the communication rights, together with democratic media governance, participation in one's own culture, linguistic rights, rights to enjoy the fruits of human creativity, to education, peaceful assembly, and self-determination.[31]

Most concepts are in agreement on the point that freedom of information constitutes one of the preconditions of freedom of opinion and expression; in specific, they concur in the view that unfettered access to information that provides the basis of opinions is indispensable to people's freedom to form their own views. By way of a grotesque historical counter-point, we should mention the example of the Soviets' campaign for liberalization during Glasnost: after the long decades of censorship and self-censorship, it finally became possible to criticize everything and everybody, while essential information about the fundamental processes behind the scenes continued to be inaccessible to the average citizen. In other words, while there was freedom of information in the West, there was freedom *without* information in the Soviet Union.[32]

[29] Among other things, it publishes its comprehensive annual report, the Global Survey.
[30] See Szekely 2007a
[31] See, for example: Assessing communication rights: A handbook (CRIS 2005)
[32] "Freedom of Expression Minus Access to Information Equal »Glasnost«" (Sirotkin 1997). See also Szekely 2006.

Without denying the interconnection and structural interdependence of FOI and FOE, the author does not subscribe to the idea of a universal *communication* right. For example, the notion of 'communication' cannot be applied to the freedoms of religion and conscience, and in any case, it is better to talk about *information* rights than about communication rights. Communication forms only one branch of the information operations,[33] the practicing of which may be accompanied by rights and freedoms.

At the same time, the concept of freedom of expression vis-à-vis information privacy is relatively easily manageable, both in the public thinking and within the law. The associated concepts are well-established; the legal and procedural rules related to freedom of expression have a long tradition in civil law, and in some cases in criminal law, also; and it is a familiar terrain for judges. By contrast, freedom of information represents a branch of law that stems from a relatively new area of constitutional law; its interpretation in the judicial practice has not yet been firmly established and, therefore, the quasi case law of the independent monitoring institutions plays a major role.

4.2 Archives and Privacy

In the case of archives, it is not only the freedom to access data and documents that can clash with the protection of privacy, but also the freedom to do scientific research. In their daily work, researchers of recent history routinely experience difficulties in trying to obtain free access to the archives on legal grounds related to the protection of privacy. The archives store large quantities of documents, which contain information about persons either positively identified or easily identifiable. In view of the fact that the (data protection) rules relating to the protection of information privacy only apply to living persons, this issue, complete with its legal and ethical aspects, could not have emerged in connection with people living in the 19th century or before: the personal data of the individuals mentioned in those documents have by now become part of history – and therefore also come under the freedom of scientific research. By contrast, documents dated from the 20th or 21st century mainly belong to a 'grey zone': neither the archivist nor the researcher can be certain whether these persons are still alive. To make things worse, several legal systems offer provisions for the temporary protection of information related to the deceased in legal constructions, which are codified outside the protection of information privacy or personal data; also, the data related to the deceased can usually be associated with other persons, too (for example, a widow or other family members) and, therefore, these are also regarded as their personal data.

In the majority of European countries, archival law – in tune with the archivists' concept, which primarily focuses on documents, rather than on the data they contain – has tried to resolve this complicated situation by specifying a general restriction period,[34] which must pass before the documents are made available for research. On top of that, the archival laws in some of the countries set a separate restriction period for documents containing personal

[33] For example, the generation, recording, storage, processing and reproduction of information.
[34] The various European countries specify the general restriction period between 10 and 100 years, with 30 years being the most widespread. For more details, see: Kecskemeti and Szekely 2005.

data. And to make the situation even more complicated, these definitions of the restriction period usually list a number of exemptions, which neither the law nor the archivists can get around: a consent to doing research in the documents by the person concerned (or his/her surviving relatives) overrules the restriction period. Similarly, those documents, which prior to their transfer to the archives, according to the FOI rules, have been publicly accessible, could not be barred from public access afterwards, regardless of whether or not they contained personal data (for example, personal data concerning public figures).

While the above-mentioned problems undoubtedly affect the traditional, 'historical' archives, too, the impact they have on the modern archives is far greater. The dramatic processes, which (sometimes visibly, and sometimes concealed by the traditional institutional mechanisms) have led to fundamental changes in archival practices and institutions, as well as in the accessibility of archived data and documents, raise further questions about the relationship between information privacy and accessibility. The new archival paradigm of the present era,[35] the vision of global accessibility, is accompanied by new techniques and practices. The *post-custodial archives* no longer admit documents in their material form, and therefore they cannot exert direct control over their use. According to the concept of the *document life-cycle management*, every document is 'archivable' from the moment of its creation (even though only a fragment of them ever make it to an archive), and therefore the same rules should apply to their handling throughout their life-cycle. Mass digitization, along with the documents that are originally produced in a digital format, offer the possibility of unlimited copies and accessibility through the Internet. According to the notion of *distributed storage*, digital format data and documents will be stored in thousands and millions of computers connected to the Internet, making use of their continuously changing memory capacity available at the moment. This is capped by a vision outlined by the biggest internet service providers (in the author's view, it is more of an illusion than a vision, both as far as its philosophy and its practicability are concerned), whereby in principle *every* information will be archivable, preservable *indefinitely,* and usable *anywhere, at any time* through digital technology.

The scope of the present paper does not allow us to do more than simply outline the problems and describe the present conditions. But even so, we can conclude as much as this: archival legislation and practice failed to meet expectations on two counts. First, in the realm of traditional archives it failed to come up with detailed regulations and practical procedures, which do not place impossible demands on researchers of recent historical documents on the one hand, and which do not lower the level of protection in the case of personal data on the other; and second, in the realm of networked digital technology it failed to offer practical solutions regarding the possibilities and problems of archiving and accessibility.

[35] The ramifications of a change of paradigm in the archival practice have been explored in numerous publications, including (Cook 1997). The author of this paper has drawn up a new catalogue of the various paradigms, arranged according to their most important features, with an emphasis on information. See Szekely 2007b (in Hungarian).

5. Common danger: Restrictions in the post-9/11 era

Along with other information rights and freedoms, information privacy and FOI were obliged to endure severe limitations in the period beginning with the symbolic choice of date: September 11, 2001. In the case of privacy, the continuous surveillance of citizens, i.e. the wiretappings and the analyses of personal communication, became general on the grounds of references to national security; and respecting FOI, the range of public information, which had previously been freely accessible, was narrowed down and the practice of classifying documents became broader, also on ground of national security (Roberts 2006).

However, the reasons put forward to justify the limitations, and especially its proposed scale, could, and must, be questioned. The phenomenon characterized with the help of metaphors such as surveillance society or the Panopticon has a harmful effect on the life of democratic societies not only on account of infringing our formal rights and unfavourably rearranging the power relations in the field of information, but also because of eroding our existing values. From the British sociologist Clive Norris' analysis it becomes clear that the sociological phenomenon referred to as 'risk society' shows up in the ideology of crime-fighting and crime prevention with a modified meaning and in a distorted sense: according to their interpretation, *crime* is no longer inherently associated with *sin*, which means that its handling is relegated to a statistical problem, losing its original value content. In other words, everyone is a potential criminal, and the only thing that stops people from committing a crime is the relatively high risk of apprehension. In turn, permanent surveillance can keep the risk of apprehension high; but if we assume that the only thing that stops the people doing the surveillance from committing a crime (for example, against those who are under surveillance) is the high risk of their apprehension, then they too, should be placed under surveillance and so forth. This is the logic that forms one of the ideological foundations of the surveillance society. Even when it produces good statistical results in the area of crime-fighting, this concept exerts a harmful effect on the value system of society, as well as on the distinction between normal and abnormal behaviour and on the handling of penal justice and rehabilitation.[36]

Similarly, a secretive state exerts a harmful influence on society not simply on account of infringing our formal rights and unfavourably rearranging the power relations in the field of information, but also because of the shaky grounds on which the restrictions are justified. As Alasdair Roberts has pointed out (Roberts 2007), it is not true that the extent of national security risk is inversely proportional to the volume of the information that is freely accessible – in some instances quite the opposite is true: a broadly informed public can reduce the national security risks.

There are numerous observers who question the claim that the serious restrictions actually began after September 2001.[37] They point out that the monitoring of people's private life,

[36] See for example the Chapter "Critical Criminology" of the Literature Review prepared for the UrbanEye project (McCahill and Norris 2002)

[37] ACLU's coalition letter to the US Attorney General on alerting privacy issues was signed in May 2001 (ACLU 2001); Amitai Etzioni in a post-9/11 study reported on Carnivore and other privacy-invasive electronic surveillance technologies introduced before September 2001 (Etzioni 2002); even the open letter of leading US constitutional lawyers, published in the New York Review of Books in February 2006 (Bradley et al. 2006), which criticized the

which is achieved through the use of modern information and communication technologies now available in surveillance, and which is aided by the privacy-invasive structure of Internet services forming integral part of our everyday life, had begun much earlier. '9/11' only provided the ideological justification; in other words, it exploited the political and public mood for the purpose of legislating further restrictions and securing for the risk industry huge contracts and vast sums of money in development funding.

Naturally, in an emergency situation it is possible to restrict information rights and freedoms – just as well as any other rights and freedoms – in a manner that is both legal and legitimate; in fact, since the rights and freedoms are not absolute, this is not even preconditioned by an emergency situation. But in an emergency situation, such as the fight against terrorism, the restrictions should be implemented in the same manner that applies to any temporary limitations of other rights. The main criterion of such a limitation is reversibility. Just as a curfew or the ban on the right to assemble can be lifted after the danger has passed, so the guarantees to the information rights should be restored to their former level after the threat has expired. Nevertheless, there are very few signs to suggest that the legislative bodies of the various countries or the industry controlling the handling of information would want to do that. In theory, the reversibility of FOI stands a better chance in this regard, since as soon the documents have been declassified, the information hitherto withheld from the public will at once return to the freely accessible domain. By contrast, the processes concerning information privacy seem irreversible. Once a piece of personal data have entered the all-pervading, networked information system, where it would be analysed and shared by various non-public government (and, through outsourcing, private) organizations without the knowledge or the consent of the data subjects, the latter will have practically no chance at all to contact each and every one of the various data controllers and data processors in order to discover, modify, delete or control information about themselves.

6. How to restrict informational rights: the need for a checklist

One could write a great deal about the relationship between information privacy and FOI, about the complex network, which encompasses various other rights and freedoms, as well as ideals and values, concerning the fields of information and communications. In this paper, the author has made an attempt to demonstrate that. Hopefully, this brief review has made it clear that the two concepts are, if not exactly friends, at least no foes of each other, either. In any case, the post-9/11 restrictions and the common threat to both types of information rights (and also to a number of kindred rights and freedoms) have ushered all of them to the same camp.

This common threat makes it necessary to find the common ground, the common criteria, on the basis of which information and communication rights and freedoms can be restricted in a democratic society. Naturally, such criteria already exist, and the constitution of numerous countries records them, with the detailed rules and regulations being scattered about in their legal systems. But the decision-makers, who have ordered these restrictions, and who, partly

warrantless electronic surveillance programs introduced after 2001 from a legal point of view, confirmed the existence of the problem since the late 1970s.

due to their direct interests and partly out of a shared conviction, consider the legal articles too abstract and the human rights advocates as a hindrance to their work, are usually unable and unwilling to interpret these scattered pieces of legislation as a group. Similarly, those who implement these decisions, or those who lend technological assistance in this, may come to conclude that their task in our highly specialized world and under the great social scheme of the division of labour, could be no other than the preservation of security and the protection of the community's values against the stronger side or the individual, and that the noble end to fulfil this role justifies the means of eroding the information rights and the values behind them.

In the author's opinion, the human rights advocates, the civil organizations and the experts of the field should all do away with the practice of merely saying "no" to the people who order or execute, or simply work in the service of implementing, the anti-terrorist measures, thus remaining on the defensive against them. They should also be able to prescribe the type of circumstances and the actual conditions, under which the curtailment of the information rights is *acceptable*. Neither the decision-makers, nor the executors, nor the auxiliary staff are prepared or motivated to carry out a detailed analysis of the factors that should limit them in executing their primary function. One of the reasons why their decisions have restrictive effects is quite frequently the fact that they either do not take into account the specific interconnections and system of criteria of the information rights, or only consider them at a far too general level. What seems to be needed is a simple, brief and well-structured document, some sort of a checklist, which clearly lists the conditions that decision-makers, along with everyone else, who executes these decisions or assists in their implementation, should take into account in the case of an emergency. The task of drafting such a checklist should befall on human rights advocates and people with specialist knowledge; then, at the next stage of the debate, they should engage the persons responsible for restricting the information rights, thus finalizing the elements of the list jointly. After this, the people who are involved in the curtailment of either information privacy or FOI can be held to account in the matter of compliance with the resulting document (even when it only carries the weight of a recommendation), with the hope that the restrictions will always be kept to the extent that is both necessary and sufficient, and that they will be done in a reversible manner, on the basis of legally and morally justifiable arguments.

References

ACLU (2001). Coalition Letter to Attorney General Ashcroft on Privacy Issues, May 2, 2001. American Civil Liberties Union, Center For Democracy And Technology, Electronic Privacy Information Center, Electronic Frontier Foundation, Free Congress Foundation, Law Enforcement Alliance Of America.
http://www.aclu.org/privacy/spying/15076leg20010502.html

Banisar, D. (2006). *Freedom of Information Around the World 2006. A Global Survey of Access to Government Information Laws.* London: Privacy International. http://www.privacyinternational.org/foi/foisurvey2006.pdf. Accessed 31 December 2007.

Bradley, C. et al. (2006). On NSA Spying: A Letter to Congress. *New York Review of Books,* Volume 53, Number 2, February 9, 2006. http://www.nybooks.com/articles/18650.

Communication Rights in the Information Society (CRIS) (2005). *Assessing communication rights: A handbook.* CRIS Campaign. http://www.crisinfo.org/pdf/ggpen.pdf. Accessed 31 December 2007.

Cook, T. (1997). What is Past is Prologue: A History of Archival Ideas Since 1898, and the Future Paradigm Shift. *Archivaria,* 43 (Spring 1997).
http://journals.sfu.ca/archivar/index.php/archivaria/article/viewFile/12175/13184 Accessed 31 December 2007.

Crane, P. S. [1967] (1999). *Korean Patterns.* Royal Asiatic Society Korea Branch, by Seoul Press, 1999.

Dix, A. (2001). The influence of Hungarian Freedom of Information legislation abroad – The Brandenburg example and experience. In Majtenyi, L. (Ed.), *The Door Onto the Other Side.* [Bilingual edition] (pp. 231–238). Budapest: The Office of the Parliamentary Commissioner for Data Protection and Freedom of Information.

Electronic Privacy Information Center (EPIC) (1999–2006). *Privacy and Human Rights: An International Survey of Privacy Laws and Developments.* Washington, DC: Electronic Privacy Information Center.

Etzioni, A. (2002). Implications of Select New Technologies for Individual Rights and Public Safety. *Harvard Journal of Law & Technology,* Volume 15, Number 2 Spring 2002. http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech257.pdf. Accessed 6 January 2008.

Fischer, W. (2007). Bush Administration Ramps up Secrecy. *Atlantic Free Press,* Monday, 10 September 2007. http://www.atlanticfreepress.com/content/view/2363/81/. Accessed 6 January 2008.

Kecskemeti, Ch. & and Szekely, I. (2005). *Access to archives. A handbook of guidelines for implementation of Recommendation No. R (2000) 13 on a European policy on access to archives.* Strasbourg: Council of Europe Publishing.

Louis, C. (200?) Freedom of Information is the flipside of Data Protection. http://www.rechtsanwalt-louis.de/foia_&_data_protection_law.htm. Accessed 5 January 2008.

McCahill, M. & Norris, C. (2002). Literature Review, UrbanEye project, Working Paper No. 2, March 2002. http://www.urbaneye.net/results/ue_wp2.pdf. Accessed 31 December 2007.

Pitt-Payne. T. (2007). Freedom of Information and Data Protection: Creative Tension or Implacable Conflict? A Paper for the Franco-British Lawyer's Society Conference, Inn of Court Northern Ireland 27/28 April 2007. http://www.franco-british-law.org/pages/ENG/publications/documents/Pitt-Payne.pdf. Accessed 6 January 2008.

Roberts, A. S. (2001). Structural pluralism and the right to information. *University of Toronto Law Journal,* 51.3 (July 2001), 243–271.

Roberts, A. S. (2006). *Blacked out: Government Secrecy in the Information Age.* New York: Cambridge University Press.

Roberts, A. S. (2007). Transparency in the Security Sector. In Florini A. (Ed.), *The Right to Know. Transparency for an Open World.* New York: Columbia University Press.

Shou, C. D. et al. (2002). *Comprehensive Information Assurance Dictionary (Draft).* National Information Assurance Training and Education Center, Idaho State University. http://security.isu.edu/NIATECV30d.pdf. Accessed 6 January 2008.

Singleton, S. (2002). The Freedom of Information Versus the Right to Privacy. A Pro-Market Framework for Arizona. *Arizona Issue Analysis 171,* May 24, 2002. http://www.goldwaterinstitute.org/Common/Files/Multimedia/35.pdf. Accessed 6 January 2008.

Sirotkin, S. (1997). Access to Public Information. In Fridli, J., Toth, G. A. & Ujvari, V. (Eds.), *Data Protection and Freedom of Information* (pp. 46–53). Budapest: Hungarian Civil Liberties Union.

Szekely, I. (2006). Freedom of information or freedom without information? The place of Hungary in the Central and Eastern European region. In Peterfalvi, A. (Ed.), *Ten years of DP&FOI Commissioner's Office.* [Bilingual edition] (pp. 261–280). Budapest: The Office of the Parliamentary Commissioner for Data Protection and Freedom of Information.

Szekely, I. (2007a). Central and Eastern Europe: Starting from Scratch. In Florini, A. (Ed.), *The Right to Know. Transparency for an Open World.* New York: Columbia University Press.

Szekely, I. (2007b). The four archival paradigms [A négy archívumi világkép]. *Információs Társadalom,* 2007. Vol. VII, No. 3, 15–46 (in Hungarian)

Theale Medical Centre (2007). Data Protection versus Freedom of Information and how it affects making an appointment. http://www.thealemedicalcentre.com/data_protection.htm. Last updated 10 January 2007. Accessed 6 January 2008.