Changing Patterns: Supplementary Approaches to Improving Data Protection

Herbert BURKERT*

I. Introduction

On May 9, 2005, Jennifer Stoddart, the Privacy Commissioner of Canada, recommended in a submission to the Senate Special Committee on the Anti-Terrorism-Act that:

> The Government of Canada should, in the context of the new national security environment, examine the adequacy of legislation that governs personal information collected, processed and shared by the Canadian government. This means a thoroughgoing reconsideration [emphasis H.B.] of the Privacy Act, of course, something that has been seriously overdue since before 9/11.[1]

In his annual report for the 2003/2004 period, the German Federal Data Protection Commissioner stated:

> (...) I am concerned about the delays in reforming the Data Protection Act. Continuous development and adaptation to a

* Dr. Herbert Burkert teaches Public Law, Information and Communication Law at the University of St. Gallen, Switzerland, where he is also President of the Research Centre for Information Law.

1 Jennifer Stoddart, "Anti-Terrorism Act" (Speech made to the Senate Special Committee on the Anti-Terrorism Act, May 2005), online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/speech/2005/sp-d_050509_e.asp> at recommendation 18.

> quickly changing environment are absolutely necessary. Later changes will be very difficult and very costly to implement.[2][Translation by the author]

These quotations provide at least anecdotal evidence that since the very first data protection act was enacted in the German state of Hesse in 1970, both the structures of general data protection laws and the filigree grid of special data protection legislation no longer meet the demands of today.

In the debate on how to improve data protection legislation we can observe a standard approach to improving data protection from a European perspective. This approach may be broken down into three schools of thought: the renovators, the reformists and the engineers (part II).

We argue that this approach is insufficient. It does not sufficiently address the fact that the deep changes of data protection's role in our information societies are neither a result of poor application of data protection laws nor a result of applying inadequate data protection laws; rather, the problem lies with parliaments continuously restricting what had been granted by the general data protection laws through special sector legislation. In order to address this phenomenon we must briefly look at the patterns of legitimacy for limiting data protection principles (part III). One of these patterns is the limitation of privacy rights by law. Parliaments have used this possibility extensively, particularly over the last five years of security related legislative activities. This observation leads to the issue of parliamentary supremacy: the possibility that parliaments can override data protection principles by subsequent laws. Checks on this kind of parliamentary power in democratic systems are classically provided by the courts.

This classical solution is insufficient. We propose a supplementary approach (part IV). This approach relies on the independent data protection agencies, and will address parliaments' role in information law

---

[2] Bundesbeauftragter für den Datenschutz. 20. Tätigkeitsbericht 2003-2004. (Presented to the President of the German Federal Parliament, April 2005), 23, online: <http://www.bfd.bund.de/information/20tb_broschuere.pdf>.

making: We argue for added transparency in law making processes as well as for a further extension of the transparency principle to provide better safeguards for data protection in the future.

II. The Standard Approaches

Current tendencies to limit the range of data protection have not gone unnoticed. There is a standard approach in opposing this trend and suggesting improvements which, at least for heuristic purposes, can be broken down into three schools of thinking: the renovators, the reformers and the engineers.

A. Renovators

The "renovators" rely on existing data protection legislation, and wish to introduce new concepts within the current frameworks and/ or shift the emphasis to hitherto neglected elements of data protection.

The German Data Protection Commissioner, in the above-mentioned quote, was referring to changes made in the German Data Protection Act which had been tabled with the responsible Minister almost four years earlier. The proposal had aimed to shift the emphasis of data protection regulation from regulating files to regulating whole systems. These systems would then become subject to voluntary or obligatory auditing procedures. The proposal had further suggested to supplement existing data protection principles (like data quality or purpose limitation) with a "minimalization principle". Such a principle would require that data holders analyze their demand of personal data more stringently, looking for alternatives to the collection of personal data, and keeping the collection of personal data, if still necessary, at a minimum. [3]

---

[3] Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka (2001): Gutachten zur Mo-dernisierung des Datenschutzrechts. Erstellt im Auftrag des Bundesministeriums des Innern, online: <http://www.staat-modern.de/Anlage/original_549072/ Modernisierung-des-Datenschutzrechts.pdf>.

B. Reformists

Like renovators, "reformists" rely on existing regulatory frameworks. However, reformists seek to reach beyond them to reconnect such regulations to underlying social and ethical values. For instance, reformists acknowledge the need for the purpose limitation and minimization principles. But they also look at the social and economic pressures which make it so difficult to maintain such regulatory principles in practice. Reformists seek to identify the interests and values underlying such pressures so as to start a reflection process on the conflicts between such interests and values and those underlying data protection. For example, they would connect the increasing collection of social security and health data with a change in our perception of distributive justice and social solidarity. In such a new value framework, diminishing means will become distributed according to individual needs, individual capabilities, and previous individual contribution. This requires more knowledge about such individual needs and contributions that can lead to an extended collection of personal data. Therefore, improvements for data protection would have to start with discussing changes in the social and political value system before returning to data protection.[4]

C. Engineers

Finally, the "engineers" assume that neither law nor the reflection of social practices alone can bring about necessary change. They see data protection largely (or at least also) as a problem of information technology which can best be addressed by that same technology. Under this train of thought, the duty to implement adequate data security had already become an important element in data protection laws; however, this emphasis still leads some to confuse data security with data protection. More recent

---

4 James Rule *et al., The Politics of Privacy* (New York: New American Library, 1980); Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder: Westview Press, 1993); and David Lyon, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (London and New York: Routledge, 2003).

activities are known under what has almost become a brand name: privacy enhancing technologies, or PETs .[5]

III. Moving to the Core: The Patterns of Legitimacy

This standard approach does not address the source of where most restrictions of data protection have come from over recent years; the source being parliaments, which have given other values more importance and legislated accordingly. This avoidance is understandable as limitations introduced by parliaments are prima facie legitimate. The political wisdom of such legislation may be criticized, elections may bring about a new parliament which might revise these laws, but the process of law making and the role of parliament is not dealt with by the standard approach.

However, the consistent trend to limit data protection principles, across party politics and national borders, calls for a supplementary approach. This approach must aim directly at the role of parliaments in legislating information flows. To better understand this supplementary approach, it is first necessary to recapitulate the patterns of legitimating restrictions to data protection as they are already embodied in general data protection legislation and the constitutional principles of data protection.

A. The Patterns

Data protection law has introduced the default rule that handling of personal data is *per se* an intrusion unless guiding principles are followed such as the purpose limitation principle, the fairness principle or other safeguards like a right of access to one's own data. The change of the default rule was justified by the potential dangers of the "new" technologies of information handling. This has been a far reaching and radical change. Its radicalism had been, and still is in some countries, one of the reasons for resisting the implementation of data protection regimes

---

5 See e.g. the contributions in: Philip E. Agre & Marc Rotenberg, *Technology and Privacy: The New Landscape* (Cambridge: MIT Press, 1997).

altogether. But with that default rule and its principles came also a broad set of justifications which would allow the handling of personal data and provide exemptions to these principles and safeguards. Data protection laws name four such reasons: consent, contract, an overriding interest, and legislation. These four exemptions formed the patterns for legitimizing the restriction of data protection. At the same time, however, all of these reasons, except one, were facing increasing criticism.

Consent, even if it is unequivocal and informed, had been a critical issue from the beginning of data protection legislation; there is a strong tendency today to discard consent under certain circumstances altogether, particularly when the data subject is highly dependent on having his or her data processed. Contracts, not only with regard to data protection but more generally, such as in the context of consumer protection, is losing its capacity to build binding obligations whenever there is at least a structural discrepancy between the contracting parties which the contract solution does not take into account. The concept of "overriding interest" is a highly case-dependent reason which is increasingly being typified by sector specific data protection legislation to make its workings more predictable. And this, finally, brings us to the fourth pillar of legitimacy: legislation.

Legislation has the possibility to modify existing data protection principles by specific laws or even to modify existing general data protection laws directly. This parliamentary override of data protection principles has become a key concern for the sustainability of data protection.

B. A Classical Problem and its Classical Solution

Laws limiting constitutional principles and fundamental rights, such as the right to privacy, point to a classical problem in parliamentary democracies, and parliamentary democracies have developed classical solutions for this problem.

Already, the designers of the first model of modern democracy realized this problem:

> "The executive in our governments is not the sole, it is scarcely the principal object of my jealousy. The tyranny of the

> legislatures is the most formidable dread at present, and will be for long years."

As Jefferson had stated in his letter to Madison of 15 March 1789.[6] Tocqueville confirmed in his analysis of democracy in America:

> « Lorsqu'un homme ou un parti souffre d'un injustice aux Etats-Unis, à qui voulez-vous qu'il s'adresse? A l'opinion publique ? c'est elle qui forme la majorité.: au corps législatif? il représente la majorité et lui obéi aveuglement; au pouvoir exécutif ? il est nommé par la majorité et lui sert d'un instrument passif; à la force publique? la force publique n'est d'autre chose que la majorité sur les armes.; au jury ? le jury c'est la majorité revêtue du droit de prononcer des arrêts; les juges eux-mêmes, dans certains état sont élus par la majorité. »[7]

Madison as well as John Locke and Charles-Louis de Montesquieu all came to the same conclusion which we find in our constitutions today: a more or less carefully balanced system of powers checking on each other. The legislative override in data protection should be read as an example of the general principle that parliaments can limit constitutional rights and freedoms, but there has to be an overriding public or private interest, the limitations have to be put into a formal law, the limitations must be proportional, and there should be a mechanism that ensures that these conditions are being met.

---

6 Letter from Thomas Jefferson to James Madison, (15 March 1789), online: First Federal Congress <http://www.gwu.edu/~ffcp/exhibit/p7/p7_1text.html>.

7 Alexis de Tocqueville (1992): De la Démocratie en Amérique volume I et II. In: Alexis de Tocqueville, Oeuvres Vol. II. Edition publiée sous la direction d'André Jardin avec pour ce volume, la collaboration de Jean Claude Lamberti et James T. Schleifer Pléiade: Paris 1992, 330f. - passim: Saage, Richard; (2005). Demokratietheorien. Eine Einführung. Wiesbaden: Verlag für Sozialwissenschaften , p.146 FN 534.

C. Parliaments, Checks and Balances and Data Protection

A Historical Reminiscence

The problem of increasing legislative limitations to data protection principles is thus a problem of separation of powers, or checks and balances in parliamentary democracies, when it comes to information and communication technologies.

The impact of information and communication technology on democratic structures and the possible role of data protection is not a new issue. The first data protection act, the Hesse Data Protection Act of 1970[8] which covered the public sector of the German state of Hesse, contained two elements addressing separation of powers issues:

- Paragraph 4 of the Act proclaimed what later would be known as the "informational separation of power", demanding that within the executive power different administrative units were not to share personal data if these units were serving different administrative purposes.
- More within the confines of the traditional understanding of the separation of powers, paragraph 6 gave the Hesse Parliament and its political groups the right to have direct access to (at that time still highly centralized) databases and programs of the Hesse executive and to have data produced according to their requirements.

These historical reminiscences, however, do not help us much with our problem. The concept of the informational separation of power has become the purpose limitation principle translated into organizational rules within the executive. It therefore does not provide a direct solution to our problem of addressing the powers of parliaments. Also, the purpose limitation principle itself is losing strength. The principle and its organizational expression are regarded to be a refusal of the very promise of increased efficiency and efficacy of information processing. The result

---

8 Gesetz- und Verordnungsblatt für das Land Hessen - Teil I - Nr. 4, Wiesbaden 12.Oktober 1970, 625ff.

is an ever increasing broadness in the description of purposes which renders the concept of the informational separation of power meaningless.

The second issue, parliament's access to data processing power, also does not address our problem directly, since it deals with increasing rather than checking on parliamentary power. It is a problem with which the technical progress and organizational changes has lost some of its urgency.

Addressing Parliamentary Override: The Role of the Courts

We are thrown back to the classical solution for checking on the power of parliaments: the (constitutional) courts. Such courts may operate on a national basis and/or on a regional basis. For example, in a European Union member state, a law relating to the handling of personal data might be tested under the jurisdiction of a national constitutional court (which would measure it against the national constitution), the European Court of Justice in Luxembourg (this court would measure such a law against European Treaty Law) and the European Court of Human Rights at Strasbourg (this court would apply the European Convention on Human Rights in individual cases and would refer to national legislation only incidentally when questioning whether national law would provide a sufficient basis for limiting a right of the Convention).

The European Convention on Human Rights is an interesting example in our context. When drafted in the late 1940s, people still had a good memory of the importance of privacy and its role to limit the reach of government power. The Convention just like its model, the Universal Declaration of Human Rights, established a right to privacy.[9] The Convention also established exemptions; it sanctioned the parliamentary override. But, within the tradition of limitations to fundamental rights and

---

[9] *Convention for Protection of Human Rights and Fundamental Freedoms*, article 8 (entered into force 4 November 1950): 8.1: Everyone has the right to respect for his private and family life, his homeand his correspondence; 8.2: There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

freedoms,, it set conditions for the limitations as well: first, a formal condition, by requiring a formal law to override the right to privacy, and second, substantive standards for any law limiting privacy to be used only for certain purposes, to be proportional and not to exceed what "is necessary in a democratic society." These limitations did not remain pure rhetoric. In several decisions the Court had to remind national administrations and legislatures of these limitations. [10]

Incidentally, the European Union, under Article 13 of its general directive on data protection, established such a limitation on limitations as well.[11] Whether the European Union's own special data protection

---

10 In one of its most outspoken decisions on that subject matter — in the case of *Klass* v. *the Federal Republic of Germany* (1978), 2 E.H.R.R. 214, the European Court of Human Rights stated — almost prophetically when we look at the current debate on national security and privacy — "(Consideration no. 49) Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."

11 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L, 23 November 1995, p. 31: *Article 13*: Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes to a necessary measure safeguard [emphasis by the author]: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others. Subject to adequate legal safeguards [emphasis by the author], in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in *Article 12* when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

legislation is observing this limitation, as in its current rule making procedures on a directive on data retention, is subject to debate.[12]

In any case, what is still lacking in Europe is comprehensive and systematic information on how courts across Europe have managed, on both the national and regional level, to check the activities of parliaments which have limited privacy rights. We also therefore lack information on how this classical instrument within the system of checks and balances has helped to safeguard, if not to improve, privacy in a changing environment.

What should also be remembered is that the courts being referred to within this system of checks and balances are courts of last resort; addressing them is time consuming and requires resources. They may function as emergency brakes, but emergency brakes, while necessary, are no substitute for a functioning regular braking system. It is this system of "regular brakes" which our supplementary approach tries to expand upon. This approach must directly address the role of parliaments.

IV. The Supplementary Approach

The supplementary approach comprises three elements: strengthening the role of data protection agencies in their relation to parliaments, modifying parliamentary procedures where they relate to legislating on (personal) information flows, and further improving rules on general transparency by extending them more explicitly to parliaments and their functions.

A. Improving the Role of Data Protection Agencies

Independent data protection agencies are a key element of data protection law in Europe. When deciding on the adequacy of national data

---

12 See the legislative opinion of the European Parliament on a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, COM(2005)0438 final, OJ C 298, 29 November 2005, p.1.

protection systems,[13] the European Commission consistently requires that such systems provide for an independent data protection agency or a functional equivalent.[14] While the actual functions of data protection agencies may vary from country to country, and their institutional structure and place in public and private sectors may differ, there are two main functions which they have to fulfill and which explain their importance in the European setting: The ubiquity of personal data processing and the fragility of the regulatory requirements against the temptations of apparent efficiency require specific emphasis on independent oversight and enforcement. And data subjects, posed as individuals against an organized data processing power, need an institutional back up to be encouraging and supportive in the use of their individual rights without being forced to seek the help of the courts directly.

Data protection agencies find themselves in a specific relationship with national parliaments. In many cases the heads of such agencies are elected by parliament, the data protection agencies may also have the obligation to report regularly to parliament, or they may have a right to address parliament on their own initiative. What seems less developed is their role in the law making process whenever data protection issues are involved. While governments may be required to involve data protection agencies in the early stages of intended legislation, in practice, even where there is such a requirement, agencies are often neglected in this proactive function.

Therefore, it seems useful to invoke mandatory participation of the data protection agency at least whenever a proposal affecting the handling of personal data is entering the parliamentary process. The law making

---

13 To profit from facilitated transfers of personal data to and from European Union countries, third countries need a formal statement by the European Commission which declares the level of data protection in that country to be adequate in relation to the level provided in the European Union (*Supra* note 12 at Art. 25(6)). For more details see <http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm>.

14 See e.g. Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, C(2003) 1731 final of 30 June 2003, OJ L 168 at considerations 8 and 12.

procedures could be amended in a way which would require that in such procedures, and at an appropriate stage, require a statement by the data protection agency to be attached to the draft. Such an obligation would at least confront law makers with the opinion of the data protection agency.

B. Addressing Parliamentary Process

The increasing amount of specific data protection regulation creates a transparency problem for data protection in general. Since it is no longer sufficient to consult general data regulations, it is becoming more difficult for the general public and for legislators to have a full understanding of the extent of data protection still available in a country. Against this background, it becomes increasingly difficult for legislators to assess the privacy impact of any new proposed legislation. Statements of data protection agencies attached to newly drafted bills as suggested above are helpful but not sufficient. The parliamentary process as such has to be addressed, and generally so.

We suggest improving the process by increasing the amount of information made available to legislators on a mandatory basis. Such improvements should apply at the "input" stage of legislation as well as at the "output" stage.

At the input stage, borrowing from the example of legislation which has budgetary implications, *all* legislation introduced in parliament should carry a "privacy impact" statement which explains what kind and which amount of personal data would have to be collected, processed and transferred once that legislation would be enacted; where this information would come from and where it would go to; whether there are alternatives to handling personal data (instead of e.g. handling anonymized information); and what kind of safeguards this legislation foresees to protect constitutional rights. As with budgetary impact statements, such an obligation would rest on all legislation to establish an effective filter to avoid legislation escaping from that information law scrutiny simply because informational impacts had not seemed to be data protection relevant. If, after such a mandatory analysis, there are no data protection impacts, the statement would say so, again similar to budget impact statements. Such information might at least alert legislators that they are dealing with a valuable resource that deserves special attention.

At the output stage, legislation passed should — as it is already the case in some countries — bear a clear mark indicating where it derogates from general data protection principles. Additionally, the respective general data protection law should carry an annex or a special schedule which — exhaustively — contains all derogations from its general principles. This indication mechanism would provide a useful transparent map for parliaments and the users of such legislation indicating what is left of the general data protection principles.

C. Improving the Transparency of Parliaments

These changes have to be embedded in a broader change aimed at improving the transparency of parliaments altogether.

This suggestion may come as a surprise. After all, if there is one democratic institution which is built on transparency, it is parliament. Sessions of parliament are open to the public, they are regularly recorded and the records are generally accessible. The election process ensures transparency of those competing to become members; and parliamentary records allow checking on the performance of those elected. So it seems consequential that regulatory reform efforts aiming at more transparency have focused on governments and administrations rather than on parliaments. It should, however, not come as a surprise that such a suggestion to improve the transparency of parliament is put forward from a European perspective. On the level of the European Union, the European Parliament has long been a neglected part of the European system of governance because of its relative lack of importance in the European rulemaking process; it took more than twenty years before members of that parliament were directly elected by European citizens, and even today this parliament has still not achieved a status in the European rule making process which would make it fully equivalent to national parliaments. Because of this slow historic process, public awareness and public scrutiny have not kept pace with the nevertheless increasing decision making power of the European Parliament. Mechanisms of public scrutiny directed at parliament are therefore underdeveloped, even if part of this lack of transparency results from the general difficulties in establishing a

general public in the highly diverse cultural and linguistic environment of Europe.

However, with the development of information and communication technology, the technological means to install and operate systems providing parliamentary transparency have improved considerably. And so have the expectations. Returning to the example of the European Parliament, while it cannot be neglected that the European Parliament has been working at improving its own transparency together with other European Union institutions[15], still far more is possible. While parliaments have been working to improve the transparency of public administrations and governments, they may have overlooked many of the potentials available for parliaments themselves. For example, the default rule of openness proclaimed for the administration should apply to parliamentary committee meetings. The network of interests in which individual members have to operate should not only be transparent to their peers but to the general public as well. Individual performance of the elected should be fully accessible to those who have elected them including the possibility to cross-reference such performances with lobbying activities.

V. Conclusion

All such measures, which have been mentioned here as examples without the intent to be comprehensive, might still not avoid the fact that parliaments can be swept away by moods of public opinion and that they might err on the constitutional limitations they too have to observe. It will still remain the task of the system of traditional checks and balances to erect barriers, even if this task is time and resource consuming.

What is happening with regard to data protection is, however, in our view, but an example of broader tectonic changes in the current

---

15 See e.g. "Communication to the Commission from the President, Ms Wallström, Mr Kallas, Ms Hübner and Ms Fischer Boel: Proposing the launch of a European Transparency Initiative" (2005) at 5-7, online: <http://ec.europa.eu/commission_barroso/kallas/doc/etik-communication_en.pdf >.

system of checks and balances caused by the development and implementation of information and communication technology. These technologies operate as power amplifiers. Changes in power structures need answers from the system of checks and balances: Which powers or checks and balances are affected by the amplification? Is the amplification distributed evenly? Where and how to intervene if this is not the case? In light of such questions, the issue of data protection and the modest suggestions which we have made may still seem to be fairly conservative comments relying on the assumption that the system of checks and balances is still basically intact. Such a position does perhaps not differ too much from approaches summarized above somewhat depreciatively as the "standard" approach. All we have really suggested with this supplementary approach is to move our attention a bit more toward what *parliaments* and not just governments are currently doing with what once had been data protection *principles* to safeguard a right to privacy. In view of the more fundamental changes which cast their shadow this modest suggestion might well prove to be insufficient in the not too distant future.