tradition. It is through the family that we inculcate and pass down many of our most cherished values, moral and cultural. * * * Ours is by no means a tradition limited to respect for the bonds uniting the members of the nuclear family. The tradition of uncles, aunts, cousins, and especially grandparents sharing a household along with parents and children has roots equally venerable and equally deserving of constitutional recognition * * *. Even if conditions of modern society have brought about a decline in extended family households, they have not erased the accumulated wisdom of civilization, gained over the centuries and honored throughout our history, that supports a larger conception of the family."

—*Id.* at 504–05.

Thus, the Court found, "the Constitution prevents East Cleveland from standardizing its children—and its adults—by forcing all to live in certain narrowly defined family patterns." *Id.* at 506. Is tradition a good constitutional argument here? Note that it is an argument often used to limit family privileges to certain people, like those who have been married in accordance with dominant religious beliefs. Do fundamental rights protect against oppressive traditions?

3. *Parental rights.* What kind of interest can be balanced against the right of parents to educate children as they see fit? Do parents exercise a family right, a privacy right, a right to collective self-determination, or a right of children that they are entitled to claim on the latter's behalf? The GCC held that the social interest in raising responsible citizens justifies certain infringements on parental and family rights. Does it? Is this a negative right against state action only, or is there also a positive obligation to educate children, or to protect them against a specific type of education, say, a very authoritarian style, or against neglect and abuse? If it is constitutional to intervene on grounds of harm, is it also justifiable on moral grounds? Also, who can claim parental rights? Consider a sperm donor, an absent father, and a surrogate mother, as well as a person who joins a family after a child was born. How important are parental rights? Can a father compel a child—or a child, a father—to undergo medical procedures for the purpose of establishing paternity? Is there a constitutional limit to a paternity claim, given that it may impose knowledge on others that they may not wish to have—on, for example, such a man's immediate family? The USSC, in *Michael H. v. Gerald D.*, 491 U.S. 110 (1989), doubted whether there is a "liberty" right to paternity that may trump the right of an active father.

E. VIRTUAL IDENTITY: INFORMATION, DATA, REPUTATION

Identity rests not only on physical appearance but also on personal history and information about one's self, thus on personal data. Where digital communication and technical devices enable us to track and save information on where people are, who they are with, and what they are doing, and where information is a commodity of high market value, the issue of personal data is of great relevance. Also, many states have, in the wake of a "war against terror," allowed police and security forces to collect vast amounts of data using surveillance techniques. Where are the constitutional limits to this? Some

issues relate to free speech (*see* Chapter 7), others to due process (Chapter 9). Here, the focus is on informational self-determination, as an aspect of autonomy and privacy. Consider this comment made already in 1987 by a scholar and former data protection officer:

> Modern forms of data collection have altered the privacy discussion in three principal ways. First, privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone. The course of the privacy debate is * * * determined by * * * the intensive retrieval of personal data of virtually every employee, taxpayer, patient, bank customer, welfare recipient, or car driver. Second, smart cards and videotext make it possible to record and reconstruct individual activities in minute detail. Surveillance has thereby lost its exceptional character and has become a more and more routine practice. Finally, personal information is increasingly used to enforce standards of behavior. Information processing is developing, therefore, into an essential element of long-term strategies of manipulation intended to mold and adjust individual conduct.
>
> — Spiros Simitis, *Reviewing Privacy in an Information Society* 135 U. Pa. L. Rev. 707, 709–10 (1987).

CENSUS CASE

Federal Constitutional Court (Germany)
65 BVerfGE 1 (1983).

[A national census gave rise to civil disobedience as people protested the state's collection of great amounts of personal data for unspecified uses. Invoking the right to human dignity in conjunction with the right to liberty, or self-determination, the Court identified a fundamental right to "informational self-determination." This right may only be infringed on the basis of a law, according to the standard of proportionality.]

It would be incompatible with the right to informational self-determination if a legal order would permit a societal structure where the citizen could not be sure who knows something about him, what they know about him, when this information can be released, and what occasions the release of this data.

"JUKI-NET CASE"

Supreme Court (Japan)
Case No. 403, 2007 (Ju) No. 454—MINSHU VOL. 62, No. 3 (2008)

1. [Appellees] allege that the collection, management or use * * * of their personal information by administrative organs by way of the Basic Resident [Registry] Network generally called "Juki-Net" * * * illegally infringe the appellees' right to privacy and other moral rights guaranteed under Art. 13 of the Constitution, and * * * by making a claim for elimination of disturbance based on such moral rights, the appellees request the appellant * * * to delete the appellees' resident certificate codes from the basic resident register. * * *

(1) Art. 13 of the Constitution provides that citizens' liberty in private life shall be protected against the exercise of public authority, and it can be construed that, as one of individuals' liberties in private life, every individual

has the liberty of protecting his/her own personal information from being disclosed to a third party or made public without good reason. [The data] consists only of the four information items (name, date of birth, sex, and address), in combination with the residence certificate code and information on change. Among these items of identification information, the four information items are personal identification information which is supposed to be necessarily disclosed in a person's social life to a certain scope of other persons. Information on change consists of the event that is the reason for change (e.g. moving-in, moving-out), the date of change, and the identification information before change, all of which cannot be regarded as highly confidential information that is related to an individual's inner mind. * * *

[T]he Juki Network can be deemed to be conducted on the basis of laws and regulations and within the bounds of the justifiable administrative purpose of improving community services and achieving operational efficiency of administrative affairs. In addition, the following facts are also found: [1] there is no concrete risk that identification information would be easily divulged through unauthorized access from outside due to system defects in the Juki Network; [2] the act of the recipient using identification information for non-intended purposes or leaking any secret concerning identification information is prohibited and subject to disciplinary action or criminal punishment; [3] the Basic Resident Register Act provides that a council for protection of identification information shall be established for each prefecture and an identification information protection committee shall be established within a designated information processing organization, thereby taking institutional measures to ensure proper handling of identification information. In light of these facts, we cannot say that the Juki Network has system defects in terms of technical or legal aspects and such defects cause a concrete risk that identification information would be disclosed to a third party or made public without the basis of laws and regulations or beyond the bounds of a justifiable administrative purpose. * * * (2) [The data collected] cannot be deemed to cause personal information to be disclosed to a third party or made public without good reason, and it is appropriate to construe that even in the absence of the consent of these individuals, such act does not infringe the aforementioned liberty guaranteed under Art. 13 of the Constitution. Also * * *, we should conclude that there are no grounds for the appellees' allegation that the management, use, etc. of their identification information by way of the Juki Network illegally infringe their right or interest in making their own decision on the handling of the information on their privacy.

TAX DATA CASE

Constitutional Tribunal (Poland)
Decision dated 24 April 1997 (K. 21/96)

[A statute allowed tax authorities to obtain information from banks on financial matters that hitherto had been disclosed only at the request of a court or prosecutor; it also allowed banks to exchange information on customers. On the premise that a legitimate interest in tax equity justified breaching fiscal and bank secrecy, it authorized certain ministerial officials to publish information about taxes paid or tax arrears of individual taxpayers engaged in commercial activity.]

Generally, it is accepted that privacy refers to the protection of informa-

tion concerning a given person, guaranteeing a state of independence where the individual may decide upon the scope and extent on his life disclosed and communicated to third persons.

[This] is a necessary element of a democratic State.

[The] right to private life also includes the protection of confidentiality of data related to the financial situation of citizens and therefore relates also to bank accounts (and similar) * * * and transactions connected with them. This especially applies to those situations where a citizen is acting as a private person and not as a business entity.

[Thus] regulation[s] permitting public disclosure of information on the amount of taxes or the outstanding liabilities may be recognized as a repressive regulation. Publication of information, even on real facts, may cause adverse consequences to interested parties, both for their business and their reputation, i.e. personal dignity. Therefore introducing the possibility of undertaking such actions towards the citizen must comply both with substantive (principle of definition) and procedural (court protection) requirements. Failure to meet these requirements must mean non-constitutionality of the regulation in question.

M.S. v. Sweden

European Court of Human Rights
28 EHRR 313 (1997)

[M.S. was diagnosed as a child as having spondylolisthesis, a condition that can cause chronic back pain. In her adult life, she slipped and fell at work, injuring her back. She was hospitalized several times and was unable to return to work for a long period. When her claim for compensation was rejected by the Social Insurance Office, her lawyer requested a copy of the file compiled by the office for the purposes of her claim. From the file she learned that the office had obtained her medical records from the clinic and based its rejection on information therein.]

32. The Court observes that under the relevant Swedish law, the applicant's medical records at the clinic were governed by confidentiality * * *. Communication of such data by the clinic to the Office would be permissible under the Insurance Act only if the latter authority had made a request and only to the extent that the information was deemed to be material to the application of the Insurance Act * * *. This assessment was left exclusively to the competent authorities, the applicant having no right to be consulted or informed beforehand * * *

It thus appears that the disclosure depended not only on the fact that the applicant had submitted her compensation claim to the Office but also on a number of factors beyond her control. It cannot therefore be inferred from her request that she had waived in an unequivocal manner her right under Art. 8(1) of the Convention to respect for private life with regard to the medical records at the clinic. * * *

37. However, * * * [t]he Court is satisfied that the interference had a legal basis and was foreseeable; in other words, that it was "in accordance with the law".

38. * * * The communication of the data was potentially decisive for the allocation of public funds to deserving claimants. It could thus be regarded as having pursued the aim of protecting the economic well-being of the country. Indeed this was not disputed before the Court. * * *

41. The Court reiterates that the protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Art. 8 of the Convention. * * *

Bearing in mind the above considerations and the margin of appreciation enjoyed by the State in this area, the Court will examine whether, in the light of the case as a whole, the reasons adduced to justify the interference were relevant and sufficient and whether the measure was proportionate to the legitimate aim pursued * * *.

42. * * * In the absence of objective information from an independent source, it would have been difficult for the Office to determine whether the claim was well-founded.

43. In addition, under the relevant law it is a condition for imparting the data concerned that the Office has made a request and that the information be of importance for the application of the Insurance Act * * *. The Office, as the receiver of the information, was under a similar duty to treat the data as confidential.

In the circumstances, the contested measure was therefore subject to important limitations and was accompanied by effective and adequate safeguards against abuse * * *

44. Having regard to the foregoing, the Court considers that there were relevant and sufficient reasons for the communication of the applicant's medical records by the clinic to the Office and that the measure was not disproportionate to the legitimate aim pursued. Accordingly, it concludes that there has been no violation of the applicant's right to respect for her private life, as guaranteed by Art. 8 of the Convention.

GASKIN V. UNITED KINGDOM

European Court of Human Rights
12 EHRR 36 (1989)

[Gaskin claimed a right to access files about his childhood that were maintained in state childcare facilities.]

38. As the Court held in [before] * * *, "although the essential object * * * is to protect the individual against arbitrary interference by the public authorities, there may in addition be positive obligations inherent in an effective 'respect' for family life."

39. The Commission considered that "respect for private life requires that everyone should be able to establish details of their identity as individual human beings and that in principle they should not be obstructed by the authorities from obtaining such very basic information without specific justification." * * * [It] noted that * * * the information compiled and maintained by the local authority related to the applicant's basic identity, and indeed provided

the only coherent record of his early childhood and formative years, it found the refusal to allow him access to the file to be an interference with his right to respect for his private life falling to be justified * * *.

40. The Government contended that * * * the present case involved essentially the positive obligations of the State * * *, [that is] a failure by the State to secure through its legal or administrative system the right to respect for private and family life. * * * [It argued there that this] entailed a wide margin of appreciation for the State. The question [is thus] whether * * * a fair balance was struck between the * * * public interest * * * in the efficient functioning of the child care system * * *, and the applicant's interest in having access to a coherent record of his personal history * * *.

42. * * * [The] Court, in determining whether or not such a positive obligation exists, will have regard to the "fair balance that has to be struck between the general interest of the community and the interests of the individual * * *."

43. * * * [It] considers that the confidentiality of the contents of the file contributed to the effective operation of the child care system and, to that extent, served a legitimate aim, by protecting not only the rights of contributors but also of the children in need of care. * * *

49. In the Court's opinion, persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development. On the other hand, it must be borne in mind that confidentiality of public records is of importance for receiving objective and reliable information, and that such confidentiality can also be necessary for the protection of third persons. Under the latter aspect, a system like the British one, which makes access to records dependent on the consent of the contributor, can in principle be considered to be compatible with the obligations under [the Convention], taking into account the State's margin of appreciation. * * * [U]nder such a system the interests of the individual seeking access to records relating to his private and family life must be secured when a contributor to the records either is not available or improperly refuses consent. Such a system is only in conformity with the principle of proportionality if it provides that an independent authority finally decides whether access has to be granted in cases where a contributor fails to answer or withholds consent. No such procedure was available to the applicant in the present case.

Accordingly, the procedures followed failed to secure respect for Mr Gaskin's private and family life * * *. There has therefore been a breach of that provision.

K.U. v. Finland

European Court of Human Rights
Appl no. 2872/02 (2008)

[Personal advertisements were posted, without a person's knowledge, on the Internet, which subjected the person to sexual advances and abuse.]

* * * 32. A comparative review of national legislation of the member States of the Council of Europe shows that in most countries there is a specific

obligation on the part of telecommunications service providers to submit computer data, including subscriber information, in response to a request by the investigating or judicial authorities, regardless of the nature of a crime. Some countries have only general provisions on the production of documents and other data, which could in practice be extended to cover also the obligation to submit specified computer and subscriber data. Several countries have not yet implemented the provisions of Art. 18 of the Council of Europe Convention on Cybercrime. * * *

40. The Court notes at the outset that the applicant, a minor of 12 years at the time, was the subject of an advertisement of a sexual nature on an Internet dating site. The identity of the person who had placed the advertisement could not, however, be obtained from the Internet provider due to the legislation in place at the time.

41. There is no dispute as to the applicability of Art. 8: the facts underlying the application concern a matter of "private life", a concept which covers the physical and moral integrity of the person. Although seen in domestic law terms as calumny, the Court would prefer to highlight these particular aspects of the notion of private life, having regard to the potential threat to the applicant's physical and mental welfare brought about by the impugned situation and to his vulnerability in view of his young age.

42. The Court reiterates that, although the object of Art. 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life.

43. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is at issue. While the choice of the means to secure compliance with Art. 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions. * * *

45. The Court considers that, while this case might not attain the seriousness of *X and Y v. the Netherlands*, where a breach of Art. 8 arose from the lack of an effective criminal sanction for the rape of a handicapped girl, it cannot be treated as trivial. The act was criminal, involved a minor and made him a target for approaches by paedophiles.

46. * * * For the Court, States have a positive obligation inherent in Art. 8 of the Convention to criminalise offences against the person including attempts and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution. Where the physical and moral welfare of a child is threatened such injunction assumes even greater importance. The Court recalls in this connection that sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims. Children and other vulnerable individuals are entitled to State protection, in the form of effective

deterrence, from such grave types of interference with essential aspects of their private lives. * * *

48. The Court accepts that in view of the difficulties involved in policing modern societies, a positive obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities or, as in this case, the legislator. Another relevant consideration is the need to ensure that powers to control, prevent and investigate crime are exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on crime investigation and bringing offenders to justice, including the guarantees contained in Art. 8 and 10 of the Convention, guarantees which offenders themselves can rely on. The Court is sensitive to the Government's argument that any legislative shortcoming should be seen in its social context at the time. * * * [But] it cannot be said that the respondent Government did not have the opportunity to put in place a system to protect child victims from being exposed as targets for paedophiliac approaches via the Internet.

49. * * * Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. * * *

Notes and Questions

1. Habeas data: Privacy, self-determination and beyond. Claims around personal data are based on a variety of rights. Which rights figure prominently in the cases above? Consider the Swedish notion of integrity as well as the German concept of habeas data as a dignity-based liberty interest, with an emphasis on citizens living in democracies. Compare this to French law, which states: "Data processing shall be at the service of every citizen. It shall develop in the context of international co-operation. It shall infringe neither human identity, nor the rights of man, nor privacy, nor individual or public liberties." Loi no. 78–17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés, § 1, and to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[hh] which refers rather broadly in Art. 1 to the goals of protection of "rights and fundamental freedoms, and in particular * * * right to privacy." In the EU, the first legal instrument to address these issues was coined as "Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," which became the global blueprint for data law. Here, we see an emphasis on privacy and data flow, in the interest of commerce. The APEC Privacy Framework, is-

hh. Convention of the Council of Europe for the Protection of Individuals with Regard to Automatic Processing of Personal Data; adopted January 28, 1981, similar to the influential 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

sued in 2005,[ii] takes a different approach, suggesting a human rights framework based on "Preventing Harm, Integrity of Personal Information, Notice, Security Safeguards, Collection Limitations, Access and Correction, Uses of Personal Information, Accountability, Choice." Note that Larry Lessig calls for moving "beyond a debate about privacy that is not really the appropriate debate in cyberspace" Lawrence Lessig, *The Architecture of Privacy*, 594.[ii] Is privacy not the correct approach?

Lessig suggests that the issue is local control of data. *See also* Anita Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 Conn. L. Rev. 861 (2000), and, for a comparative analysis, David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States 594 (1989). Also note that, in 1997, the International Labour Organization (ILO) issued a code of conduct, Protection of Workers' Personal Data, reacting to growing concerns around employers monitoring employees' computers and mail communication. Consider what Gebhard Rehm has to say:

> In some respects, the situation has become frighteningly similar to George Orwell's "1984" vision of a totalitarian state keeping its citizens under complete surveillance. That an *Orwellian* society, consisting of degrading human beings to mere objects of state action, is inconsistent with the Kantian idea of man as a rational being, that underlies a democratic society based on the rule of law, hardly needs explanation. But every single move towards a society with more rather than less surveillance also gnaws at Kant's ideal because it leads to more heteronomous decision-making. The more others know about individuals, particularly those who wield a certain power over them such as government or employers, the more the individuals will feel urged to subordinate their own judgment to that of others.
>
> —Gebhard Rehm, *Just Judicial Activism? Privacy and Informational Self-Determination in U.S. and German Constitutional Law*, 32 UWLA L. Rev. 275, 275–79 (2001).

Unlimited collection and availability of data not only conflicts with the philosophical values that are at the core of democratic societies, but also has negative legal implications. It violates the spirit of liberties that human beings enjoy in a democratic and liberal society. Surveillance of one's behavior, even the fear of being controlled, tends to have a chilling effect on the enjoyment of freedom. * * *

On the other hand, a right to protect one's data against public knowledge cannot be absolute. The discharge of governmental functions requires a solid basis of information. * * *

This conflict of countervailing interests regarding privacy did not go unnoticed by neither the German Federal Constitutional Court nor the U.S. Supreme Court. Both courts have tried to cope with this challenge by recognizing a constitutional right of each individual to control the flux of certain personal information. The Federal Constitutional Court has called this right,

---

ii. *Available at* http://www.apec.org.

jj. Paper presented at the *Taiwan Net 98* conference (Taipei, March 1998); *available at* http://lessig.org/content/articles/.

somewhat clumsily, the "right to informational self-determination," [*Census Case*] the U.S. Supreme Court subsumes this right under the right to privacy. The constitutional right to privacy encompasses, however, the protection of basically two interests: firstly, the individual interest in avoiding the disclosure of personal matters (the "informational aspect"), and secondly, the interest in the independence in making certain kinds of important decisions (the "decisionmaking aspect") [*Whalen v. Roe*].

* * * [T]he differences in structure, scope and level of protection between the right to informational self-determination and the right to privacy are by no means negligible. The German Federal Constitutional Court has derived a comprehensive right to privacy from the right to personhood which is guaranteed in Art. 1, 2 GG. The U.S. Supreme Court, in contrast, has refused to recognize an all-embracing right to privacy as a matter of federal constitutional law that in principle protects against disclosure of any data. * * *

2. Erase Data. In many instances, people want their data to disappear, often, from police and security forces files. How could one construe a fundamental right to erase data from state files? Do they extend to private actors, like an internet provider? In Canada, the Supreme Court held that retaining a juvenile first-time offender's DNA sample on the national data bank is grossly disproportionate. *R v. RC,* [2005] 3 S.C.R. 99, 2005 SCC 61 Referring to an earlier decision (*R. v. Plant*), the Court emphasized the protection of the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state." Since an individual's DNA contains, the Court argued, the "highest level of personal and private information," and is "capable of revealing the most intimate details of a person's biological makeup," to take and retain such data can only be based on a compelling public interest, since it interferes with a "right to personal and informational privacy." *Id.* The ECtHR, in *S. and Marper v. UK, Appl. nos. 30562/04 and 30566/04* [2008] also emphasized proportionality when keeping DNA and fingerprints for crime prevention. It applied the concept of "private life" as developed in *Pretty*, discussed above, to "embrace multiple aspects of the person's physical and social identity." *Id.* The Court listed "gender identification, name and sexual orientation and sexual life" as well as a person's name and other means of personal identification and of linking to a family, data on a person's health, an individual's ethnic identity and one's image. It argued that "bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today." *Id.* at para 71. The Court also emphasized that DNA used to register a person's ethnic background is subject to particular scrutiny, and that fingerprints, in light of today's technology, are analogous to photographs or voice samples, and should be subjected to similar scrutiny.

3. Access to government data. Many courts have recognized a right to keep data or to have data erased, but courts also acknowledge a right to obtain data. The Panama Court, in *Cochez Farrugia v. Ministry of the Presidency,* Habeas Data on Appeal, Record No 47s, HD 272-2002, described a right of access to data as a right to informational self-determination, a third generation human right stemming from privacy. In Peru, the Constitutional Court

emphasized that citizens have a right to obtain access to government data, regardless of their reason for requesting it. *Rodriguez Guiterrez v. Paniagua Corazao*, Exp No 1797-2002-HD/TC. This extends to information about the president's annual travel expenses. *Rodriguez Guiterrez v. Toledo Manrique*, 0959-2004-HD/TC. In India, the ISC understands access to government information as an issue of freedom of speech (*S.P. Gupta and Others v. President of India*, A.I.R. 1982 S.C. 149, 234), in an analysis similar to that of the Israeli Court in *Shalit et al. v. Peres et al.*, 44 (3) P.D. 353 (1990). What if data a government keeps does relate to the private lives of individuals? The USSC has held that there is a common law right "to inspect and copy public records and documents, including judicial records and documents." *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 597 (1978). However, "[e]very court has supervisory power over its own records and files, and access has been denied where court files might have become a vehicle for improper purposes." *Id.* at 598. From a perspective of fundamental rights, what is "improper"? The USSC, discussing access to an individual's criminal record, drew a distinction between access in the interest of targeting a private person (by reporting in mass media, for example) and access in the interest of monitoring the government (in a context such as civil rights activism). *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989). The ECtHR, in *Guerra v. Italy*, 26 EHRR 357 (1998), held that citizens may have a right to public data if their health is endangered. There is also a long Swedish tradition (dating back to 1766, when Sweden adopted its Freedom of Information Act), allowing for broad access to public files, that has come, gradually, to inform the laws of other EU member states. For example, in 1999, the Czech Republic passed the Free Access to Information Law (Act no 106/1999), under which all citizens have the right to be provided with information by state and local administrative bodies, with exceptions for classified information, business secrets, and personal data. If such rights are fundamental, may they still be limited in order not to compromise investigations, as when states try to identify "sleeper cells" of terrorism?

4. Contexts. The right to anonymity has been conceived as the informational aspect of the right to privacy, translating into a right to control the use of personal data and a policy of data protection. While it has been accepted in many jurisdictions, as in Puerto Rico (*Lopez Vives v. Policía de P.R.*, 118 P.R. Dec. 219 (1987)), scholars observe that "privacy is minimal where technology and social organization are minimal". Barrington Moore, Jr., Privacy: Studies in Social and Cultural History, 276 (1984). Is a right to personal data not a universal human right? Or does this imply that a lack of developed schemes of data protection law in some Asian and African countries, when compared to many states in Europe and North America, indicates a particular state of technology, rather than a cultural trait? But note that the U.S. does not employ the means of data protection common in Europe. How can one explain such differences? Scholars have argued that they "can be attributable to differences in perceptions of the degree to which privacy is or will be threatened," and that "the comprehensive, bureaucratic nature of data privacy regulation in Europe undoubtedly reflects traumas from relatively recent, firsthand experience there of totalitarian oppression." Engaging Privacy and Information Technology in a Digital Age, 377 (James Waldo, Herbert S. Lin, and Lynette I. Millett, eds., 2007) Consider that the GCC emphasizes the importance of

knowledge as part of informational self-determination. Is this related to a particular vision of democracy? And if so, does a right to one's data extend to public as well as private actors, like, say, a university taking surveillance videotapes, or should standards differ regarding the state and private actors? Often, signs tell people there is a camera somewhere. Does that legitimate an interference with fundamental rights? Does one consent to a collection of personal data by using an online search engine or social networking site, or an e-mail account? The ECtHR held in 2009, in *Iordachi et al v. Moldova* (Application no. 25198/02), that "the mere existence of legislation [which allows for phone tapping] entails, for all those who might fall within its reach, a menace of surveillance." In Moldova, there was evidence that the state surveilled human rights lawyers. Does the political context make a difference to doctrinal standards of dignity, or privacy? In a landmark decision from Germany, the *Eavesdropping Attack Case*, 1 BvR 2378/98, the GCC held in 2004 that a counter-terrorist surveillance law that allowed police to bug a private home violates fundamental rights. It referred to human dignity as an inviolable right to an "absolutely protected core space of the private design of one's life" ("*absolut geschützten Kernbereichs privater Lebensgestaltung*") as a foundational pillar for the rule of law in all phases of data usage in criminal proceedings. Note that the GCC has held that medical records (32 BVerfGE 373, at 379 (1972), fall outside the "core." Compare this to the Swedish case above. Consider that the USSC held, in *Chandler v. Miller*, 520 U.S. 305 (1997), that drug testing as a means to obtain medical data on a person is not constitutionally valid when designed as an entry requirement for public office. The GCC now seems to argue that the home is protected regardless of the state's reason for investigating it. What concept of dignity informs this argument? Could one reach similar conclusions based on privacy, or self-determination?

5. Transitional justice. Conflicts around informational privacy or self-determination often rise in contexts of political transition, as in postcolonial, post-dictatorship as well as postsocialist contexts. People may want to know what happened in the past. In Argentina, the Supreme Court ruled that an individual had a right to know where his brother was taken by the secret police, *Urteaga v. Estado Mayor Conjunto de las Fuerzas Armadas*, Argentina Supreme Court, [1999-I] J.A. 22. Is this a reaction to a specific historical situation, or a universal right? Also, societies may have a cognizable interest in knowing what people did in positions of power in a former regime. In postsocialist Hungary, the Constitutional Court held in the 1994 *Lustration case* that an act mandating background checks on individuals holding certain key offices violates their constitutional rights. However, it stated that "data and records on individuals in positions of public authority and those who participate in political life—including those responsible for developing public opinion—that reveal that these persons at one time carried out activities contrary to the principles of a constitutional state, or belonged to State organs that at one time pursued activities contrary to the same, count as information of public interest." Nonetheless, the Court held that law must meet a certain standard if it is to allow such data to be revealed:

> 'Lustration laws' * * * are typical products of the change of system underway in the former socialist countries of East-Central Europe. The lustration, or background checks, generally served two different purposes, and accordingly, the laws come in two types. The majority of lustration laws

lay down rules on incompatibility. Those who held certain State or party positions in the former socialist system, and further, those who belonged to the ranks of the political police or were to be found among its secret informers, may not occupy certain positions as the change of system unfolds. Particular laws extend to employees of institutions of culture, (higher) education, and academia, public service radio and television, and also to lawyers (see the Czech and Slovak lustration or purification law of 1991, and the * * * 1990 treaty uniting * * * Germany * * *, [and the] laws * * * in Bulgaria [and] Albania). Constitutional Court decisions were rendered on each of these acts in the respective countries. * * * [T] he constitutional complaints concerned violations of the right to freely choose employment and occupation, and of international agreements which guaranteed social welfare rights.

A consummate example of the other type of lustration law is Germany's 'Stasi Act.' In this case, the primary aim was nothing other than bringing completely to the light of day the activities of the former State security organs and secret agents. Calls for the public naming of former agents were to be heard in other countries as well, but did not come to pass. * * *

The 'lustration' or background check thus came in two types, according to purpose. One aimed to guarantee personnel replacements in certain key positions, and at the same time keep the nation's transition as defined in the Constitution from being endangered by those who in the past stood actively and in their professional capacity against the principles of a constitutional state. The other aimed toward a genuine public disclosure of the nature of the previous regime, to guarantee a measure of redress, and simultaneously to symbolise the irreversibility of the changes, through revealing the activities of the secret services.

* * * [T]he Act at issue * * * was created with the same purpose. * * * [But] it can not be said * * * that it aims primarily to avert a suspension of or risk to the transition. Nor was the identity of the one-time agents publicly disclosed; indeed, the post-socialist era legislative process only broadened the veil of secrecy. * * * Even the content of the Act differed from that in other countries; it neither declares incompatibility between personnel in past and present offices, nor proposes to unveil the whole previous system of political informing, least of all with respect to those who had been under observation. The Act in fact promotes the transparency of those in prominent political and other public roles, and thus of the life of the nation in general. In it, there is a confluence of the moral obligation that remained in the wake of the transition: the unveiling of deceit, publicity rather than punishment and the value system normal to a constitutional state.

The Act must therefore be examined in view of present-day, normal legal conditions characteristic of a constitutional state. Owing to the passage of time, the legal peculiarities of the transition period can today hardly be validated within the framework of obligations presumed by a constitutional state. It must also be taken into account, however, that the change of system, from a political perspective, in fact marked a revolutionary change in that prior to the Constitution, Hungary was by definition not a constitutional state. * * *

The Act must therefore be examined in view of the fact that in a consti-

tutional state, the fundamental right to the freedom of information presumes that the functioning of the State is transparent to its citizens. For this reason, the scope of private life of individuals who hold positions of public authority or who partake in political life—with respect to aspects in connection with these public activities—is restricted. Entirely independent of the original goals of the lustration laws, "public" information on individuals in certain positions of public authority today necessarily includes information revealing previous activity expressly contradictory to the principles of a constitutional state, or individuals' memberships in an organization which pursued such activity. In defining the range of such activity, the Constitutional Court must consider the transition as a historical fact. * * *

Nor can it be overlooked that the very system of records at issue, maintained to the present day, is itself unconstitutional, and that these records both those of the agents who supplied the information, and those of the individuals who are the subjects of the files must therefore be brought into harmony with the Constitution. Continued secrecy, constitutionally speaking, is an insufficient solution. * * *

The shedding of light on the past, and with it an objective evaluation of the importance of the change of regime, presumes the public disclosure of the activities of the former secret services. With regard to such records, even laws which otherwise protect the security of information, personal and otherwise, regularly make exceptions to the rule, given suitable guarantees and in order to serve the interest of public knowledge. * * * Just as violations of the right to (informational) self-determination require clarification of just who may gain access to secret service files which concern them, so that they may understand the true extent to which the past regime influenced their personal fate, and in this way, at least, temper the transgression against their human dignity, so too the nagging issue of the past in the larger sense, as it concerns the nation as a whole, can be resolved only if the secrecy of former secret service records is not further maintained.

[But an] unconditional secrecy of the data in the records * * * is unconstitutional * * *

The fundamental right to the protection of personal records and to access information of public interest are properly interpreted in light of each other. * * * This is natural, for informational self-determination and the freedom of information are two complimentary preconditions for individual autonomy. * * *

—*Lustration case* (Decision 60/1994 (XII.22.) AB hat.[kk]

6. Technology at work. The HCC demanded safeguards against unlimited data transfer, based on an argument similar to the German decision in the *Microcensus Case*, 27 BVerfGE 1 (1969). However, much technology is deliberately designed not to allow for such control. Should the law have a say in the design of technology, or does the structure of technology itself constrain the law? In *Intel Corp. v. Hamidi*, 114 Cal. Rptr. 2d 244 (Cal. Ct. App. 2001), the USSC held that limitations of communication on a corporation's e-mail system were not protected as free speech, since such a system

kk. Reproduced from 2 E. Eur. Case Rep. Const. L. 159 (1995).

was seen as a private, and not public, forum. Connection to the Internet, the Court found, does not render it a public space. Does that impose constructive requirements on technology?

7. Public and private. A large percentage of data is processed by private rather than by public actors. Are there fundamental rights to dignity, or privacy, at the workplace? Do such rights include rights of access to data, and to have them erased? Consider the view of Lawrence Rothstein::

> [In the U.S., privacy] highlights a "possessive individualism." Privacy implies notions of property, individualism, ownership and expectations with regard to the exclusion of outsiders without specific legal rights to the work premises. * * * Privacy is associated with one's home, with intimate relations, and with premises under a person's control. * * * This possessive, territorial view of privacy finds clear expression in the workplace.
>
> When a worker sells her capacity to labor, she alienates certain aspects of the person and puts them under the control of the employer. Thus in the U.S., workers in the workplace, except occasionally in restrooms and employee locker rooms, are not generally protected from surveillance on the grounds that the premises and equipment are possessions of the employer and the employee can have no legitimate expectation of intimacy or of protection from employer intrusion.* * *
>
> Where Anglo-American jurisdictions emphasize the concept of privacy in their legal protection of workers from monitoring and surveillance, continental European countries manifest a concept of human dignity more related to notions of community and citizenship than property. French, Italian, German and Spanish do not even have a direct equivalent of the English word "privacy." The concept of human dignity is a social one that promotes a humane and civilized life. The protection of human dignity allows a broader scope of action against treating people in intrusive ways. * * * At work, human dignity is denied by treating the employee as a mere factor of production with fixed capacities and vulnerabilities determining her behavior and ignoring both the worker's individuality in the face of statistical probabilities and the human potential to overcome or compensate for physical obstacles. The worker's dignity is denied when she is treated as a mechanism transparent to the view of others at a distance and therefore manipulable or disposable without the ability to confront the observer.
>
> [The author describes French and Italian labor laws and concludes:] In France and Italy, unlike the U.S., there is legal recognition that private power is as much an attack on dignity and liberty as is public power.

—Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. Sch. J. Int'l & Comp. L. 379, 382 (2000).

8. Anonymity. If there is a right to decide about personal data, is there also a right to use, or to withhold the use of, say, one's name? Consider the ECtHR decision against Norway. Meanwhile, a U.S. district court, in *A.C.L.U. v. Miller*, 977 F.Supp.1228 (N.D.Ga., 1997), decided that an act that made it a crime for any person knowingly to transmit false or unauthorized personal data through a computer network, infringed on protected speech that might have the purpose of avoiding social ostracism, preventing discrimination and

harassment, and protecting privacy, and was not drafted with the precision required for laws regulating speech. While recognizing the constitutionality of such provisions under certain circumstances—such as efforts to prosecute persons who falsely identify themselves with the intention of deceiving or defrauding the public, or persons whose commercial use of trade names and logos creates a substantial likelihood of confusion or the dilution of a famous mark, the court nevertheless found the challenged statute overbroad because it operated unconstitutionally for a substantial category of the speakers it covered. The USSC, in *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995), decided that a prohibition against the distribution of anonymous leaflets was not constitutionally valid. Is there a difference between the distribution of information on the Internet and on the street? Whose fundamental rights are at stake, the speakers or the people being spoken about? Consider that German courts do not release names of people involved in cases when they publish decisions, while North American courts do. What if court hearings disclose personal data of people with only incidental or tangential involvement in cases? Should it matter how "private" or "intimate" such data is, and from which perspective should this be defined? Consider an argument by the ECtHR, in *B. and P. v. United Kingdom*, 34 EHRR 19 (2002), in which a judge closed a custody hearing to the public. When the fathers who sought custody claimed that this violated their right to a fair trial, the Court responded:

> [The] requirement to hold a public hearing is subject to exceptions. This is apparent from the text of art 6(1) itself, which contains the provision that "the press and public may be excluded from all or part of the trial * * * where the interests of juveniles or the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice." [In the present case the] applicants [had sought to hold in public proceedings that] concerned the residence of each man's son following the parents' divorce or separation. The Court considers that such proceedings are prime examples of cases where the exclusion of the press and public may be justified in order to protect the privacy of the child and parties and to avoid prejudicing the interests of justice. To enable the deciding judge to gain as full and accurate a picture as possible of the advantages and disadvantages of the various residence and contact options open to the child, it is essential that the parents and other witnesses felt able to express themselves candidly on highly personal issues without fear of public curiosity or comment.

9. Reputation. Privacy and dignity concerns often arise when people feel their reputation is ruined. This may apply even to the deceased. The German GCC held that a novel that "dishonors the good name and memory of a now-deceased famous actor" could be banned to protect personality rights, given the dignity interest involved (*Mephisto Case,* in Chapter 7), when the actor was portrayed as deeply involved with the Nazis. In 2000, in the *Burial Ground* case, the Constitutional Court of Macedonia stated:

> Safeguarding human dignity is a fundamental human right and a precondition for implementing humanity, a fundamental principle of the constitutional order. Human dignity does not relate only to living people; its protection also covers deceased persons. Making it a crime to place photographs, statements or other memorial on the tomb of deceased persons

who were enemies during World War II or enemies of the social and political system of the Republic, infringes the right to be buried in a normal, decent way. It also violates without justification fulfilment of the moral duty of persons related to the deceased to bury a relative in such a way.

—U.br. 32/2000, Sluzben vesnik na Republika Makedonija [Official Gazette] 79/2000).

Does this mean that a right to dignity extends beyond death and implies an obligation of relatives? More frequently, claims are brought by those who are still alive. In Italy, a doctrine of a "right to personal identity" is associated with the *Pretura Roma* case (Pangrazi and Silvetti v. Comitato Referendum, Giurisprudenza Italiana, 1975, I, 2, 514). brought by a couple whose photograph was used without their consent in a political campaign they did not support. In *von Hannover v. Germany*,40 EHRR 1 (2004), the ECtHR held that newspaper publication of photographs of a prominent person's daily routines violated her privacy right, stating: "the fundamental importance of protecting private life from the point of view of the development of every human being's personality. That protection—as stated above—extends beyond the private family circle, and also includes a social dimension * * *" Para. 69. Should it make a difference to rights of dignity and privacy how famous people are, or what they do? Note that the Australian Supreme Court of NSW rejected a claim by a medical practitioner against a newspaper that published his picture and name. Levine J stated:

[The] right to privacy with which this case is concerned does not involve that area of "data protection". What it does involve is the focus upon the simple relationship between an individual in the community to whom reference is made in the media and the media itself as a component of society, its accountability, the astonishing power of the technology available to it for the dissemination of information and the immediacy thereof. The current applications would not be an appropriate vehicle for the resolution of all the problems attendant upon the question of the "right to privacy" as understood in the community generally, as the subject of Art. 17 in the International Covenant on Human Rights [*sic*] and, in light of the structure of my rulings thus far, as a matter of substantive law.

—*"GS" v. News Ltd* (1998) Aust Torts R 181–466.

Consider that the USSC, in *Connecticut Dept. of Public Safety*, 538 U.S. 1 (2003), held that registrants do not have a due process right to attend a hearing designed to determine their threat level to society. It found that "mere injury to reputation, even if defamatory, does not constitute the deprivation of a liberty interest."

10. Type of data. Should fundamental rights protection vary according to the type of data—medical, business, or intimate, for example—at issue? Compare *M.S.* and *Gaskin*: Is there a decisive difference? In *Yesimhovitz v. Baruch and Bros.*, 447/72, 27 (2) P.D. 253 (1973), the Supreme Court of Israel held that disclosure of medical records for tax purposes does not violate the Constitution and that there is no duty of confidentiality for doctors when a patient discloses an illegal act. Consider this comment:

Notably, the differences between Israel and the United States regarding the disclosure of medical information relating to possible violent acts do

not necessarily reflect a greater respect for medical secrecy in the United States. Rather, Israel's more expansive exceptions can be attributed to cultural and societal differences between the two countries, which are unrelated to the doctor-patient relationship. Indeed, it is difficult to compare a society of five million people with a compulsory army and large portions of civilians carrying weapons, with a society with almost 300 million people with a voluntary army and more unlicensed guns than licensed guns.

—Silverstein, Steven, *Medical Confidentiality in Israeli Law*, 30 J. Marshall L. Rev. 747, 755 (1997).

Consider that data on bank accounts has for a long time been considered very private and thus protected. Is it compatible with constitutional protections of privacy to release such information to the public or to police investigators to prevent, for example, money laundering or the financing of international terrorism? Anita Ramasastry, *Secrets and Lies? Swiss Banks and International Human Rights*, 31 Vand. J. Transnat'l L. 325, 341–42 (1998). In Belize, the Supreme Court held in *SEC v. Swiss Trade*, [1995] (Belize) (No. 85) that data kept by private companies is protected not merely in terms of maintaining confidentiality but also in the context of protection from foreign investigators (in this case, from U.S. officials). Can and should constitutions protect against transnational searches? Consider the extradition cases discussed in section C.1. What about "intimate" data? A U.S. state supreme court held, in a case concerning private pictures of a person in a shower: "One's naked body is a very private part of one's person and generally known to others only by choice. This is a type of privacy interest worthy of protection. Therefore, without consideration of the merits of [the] claims, we recognize the torts of intrusion upon seclusion, appropriation, and publication of private facts." *Lake v. Wal-Mart*, 582 N.W. 2d 231 (Minn. 1998). Is there a type of privacy interest that does not deserve protection? Consider the use by security personnel at airports of body scanners, similar to x-rays, which was discussed in Europe as a violation of dignity. The USSC held, in *Smith v. Doe*, 538 U.S. 84 (2003), that the Alaska Sex Offender Registry was constitutional because it held data that was already in public criminal records, and that giving this data to communities is not excessive, given that people in the U.S. often relocate. Justice Stevens, however, acknowledged in a concurrence that dissemination of such data is harmful in many ways to those on the registry. In France, and also in Italy, for example, there is legal recognition of a "*droit de l'oublié*," a right to forget and a right to silence concerning one's criminal past. What reasoning protects fundamental rights best?