Access to and Use of Publicly Available Information

A

Philip Leith
Queen's University of Belfast, UK

INTRODUCTION

Public information presumes that the information is somehow public and, presumably, that this can be utilized by members of the public. Unfortunately, things are more complex than this simple definition suggests, and we therefore need to look at various issues relating to public information which limit access and usage, for example, the nature of privacy, sharing information within government, court records, ownership of public information, and freedom of information. The exemplars dealt with later in the article will demonstrate the legal constraints upon the usage of public information in a digital environment and help raise awareness of such limitations.

Public information cannot be formally defined (as a list of items, say) except to indicate it is that information which has historically been available to the public in print form and/or through some generally open process. No formal definition is possible because this depends to a very large extent upon cultural differences. For example, tax returns are viewed as private documents in the United Kingdom open only to the tax authorities (unless otherwise authorized, e.g., in criminal proceedings) whereas in Sweden they can be accessed by any member of the public. Furthermore, the source of public information may also vary: what information is produced by a public authority in one country may not be so carried out in another.

The legal constraints upon access and use of public information include the following:

- Privacy/confidentiality of public data
- Sharing and processing of public data collected for divergent purposes
- Freedom of information rights to public data
- Copyright and database rights in public data

Access to public information may be enabled through a formal public register, through statutory mechanism, or other less formal means. Note that being accessible does not necessarily mean that users are free to use this information in any way they wish: copyright licenses in particular are not always passed along with access rights, so that the public may inspect a document but may not use it in other ways (such as republishing). Reasons for this are obvious: the collection of data by government can be expensive and there can be opposition to subsidising commercial activity from the public purse. In the United States, federal materials are explicitly excluded from copyright protection, but this is rarely the case in Europe (see www.hmso.gov.uk for the UK situation).

Another example is that it is possible in most countries to attend local criminal courts or peruse local newspapers and draw up a database of prosecutions in the local area. The database could include information on drunk drivers, sexual offenders, and burglars, and it would be possible to include a wide variety of information—all of it, clearly, of a public nature. Indeed, such activities have been common for many years where credit agencies have collected information from courts on debtors and made this available on a commercial basis. But there are questions: Is all court-based information public? What limitations might be found in some countries and not in others to the dissemination of this information? See Elkin-Koren and Weinstock Netanel (2002) for the general tendency toward commodification of information and Pattenden (2003) for professional confidentiality where it impinges upon public service.

On a more mundane level, judgments from most European courts are copyright of the relevant government or agency. In the United Kingdom, differing again, there is some dispute over whether the judge or Court Service owns the judgment, and frequently the only text version of a judgment is copyright of the privately employed court stenographer.

Thus the publicly available information which is being discussed here is that which emanates from a public authority and can be accessed by members of the public, but will usually have some constraint and limitation on how it can be reused by the public. We are interested in outlining these constraints.

BACKGROUND

Much of what has driven recent legislation concerning publicly available information has been fear of the differ-

ences between print access and digital access—particularly that of ease of access and length of period of access. Even in 1972, the Younger *Report on Privacy* (1972) noted that there was concern discovered in their research over the usage of computers for the collection of data when there were 4,800 computers "in use or on order." The situation has become much worse—to the privacy advocate—since the inception of the Internet and a freefall in the price of storage. Access to information is global and with the rise of systems such as Google's caching mechanism and the *waybackmachine* (www.waybackmachine.org). Once information has been put onto a Web server, it can be difficult to remove it from public view.

In the case of *Lindqvist*, we can see the legal system is having difficulties in treating these new developments as a natural growth from print technologies. Mrs. Lindqvist set up a parish Web site for her church which noted that a member of the local community had hurt his foot. She was prosecuted by the Swedish Data Inspection Board for failure to register her processing of personal data and for revealing sensitive personal data about the owner of the hurt foot. She was also prosecuted for transferring this to third countries by making it available on the Internet. The case was referred to the European Court of Justice (ECJ) for clarification on various matters relating to data protection. The court found that

The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data.... Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health. ... (Case C-101/01, Judgment November 6, 2003)

However, it did not find that Web publishing was transferring this information to third countries. This decision shows the ECJ's perspective on two fronts. First, it shows that it holds that medical information on the individual should usually be protected from data processing unless permission exists; and second, that it sees a distinction between whether Mrs. Lindqvist had produced her local gossip in print or in digital form. This latter point is important: we can expect less and less material to appear in print rather than digital format, so a practical pressure is being applied by data protection law to change the nature of communication within local communities, as well as within the national or international sphere.

It is in this quirky context that European access to digital public information must be viewed.

THE PUBLIC/PRIVATE DIVIDE IN A DIGITAL ENVIRONMENT

There is much information that is publicly available but that can potentially be problematic in a number of ways when we move into a digital environment. It is clear that this public information access can sometimes be viewed as undesirable: the information is certainly public, but when it is print based it can be difficult to access and—except to the industrious researcher—tends to be hidden from public view. In particular, this is information that relates to a particular individual—say his or her criminal record, ownership of property, grants received from government, his or her tax return, and so forth. In a digital e-government environment the public nature tends to become magnified simply by the ease of storage, processing, and access.

A second kind of public information is that which the public may have a right to know and access in order to ensure that a public authority is carrying out its tasks properly and effectively. Such information is subject to freedom of information legislation (see Birkinshaw, 2005) in many countries. Much of this pubic information necessarily touches upon private information—letters/e-mails from citizens to public authorities, data collected as part of everyday government tasks, commercially sensitive information. Where should the line be drawn between what is public and what is private?

At the heart of the question of what is public and what is private is the philosophical debate over the nature of government, the role of the citizen in government, and the role of government in overseeing proper standards of the citizen's behaviour. Classical theories are well known in the literature and certainly have had effect upon the development of legislation. However, such abstract theories are difficult to put into practice and the legal texts have most usually lacked clarity for obvious reasons. For example, *The European Convention on Human Rights* gives weight to private life in Article 8 (1):

Everyone has the right to respect for his private and family life, his home and his correspondence.

But immediately constrains that right in Article 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.