INTERNATIONAL CONFERENCE OF DATA PROTECTION &
PRIVACY COMMISSIONERS

RESOLUTION ON RADIO-FREQUENCY IDENTIFICATION

Final Version

20 November 2003

Following a proposal by the Data Protection and Access to Information Commissioner Brandenburg, the Independent Center for Privacy Protection Schleswig-Holstein, Germany, the Spanish Data Protection Agency and the Data Protection Commissioner of the Canton Zug, Switzerland, the International Conference resolves that:

Radio-frequency identification (RFID) technology is increasingly being deployed for a variety of purposes. While there are situations in which this technology can have positive and benign effects, there are also potential privacy implications. RFID tags are so far primarily used to identify and manage objects (products) to control the supply chain or to protect the authenticity of the product brand; however, they could be linked with personal information such as credit card details and even used to collect such information, or to locate or profile persons possessing tagged objects. This technology could allow for the tracing of individuals and for linking collected information with existing databases.

The Conference highlights the need to consider data protection principles if RFID tags linked to personal information are to be introduced. All the basic principles of data protection and privacy law have to be observed when designing, implementing and using RFID technology. In particular

a) any controller – before introducing RFID tags linked to personal information or leading to customer profiles – should first consider alternatives which achieve the same goal without collecting personal information or profiling customers;

b) if the controller can show that personal data are indispensable, they must be collected in an open and transparent way ;

c) personal data may only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve (or carry out) this purpose, and

d) whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags.

These principles should be taken into account when designing and using products with RFID.

The remote reading and activating of RFID tags, without any reasonable opportunity for the person in possession of the tagged object to influence this process, would raise additional privacy concerns.

The Conference and the International Working Group on Data Protection in Telecommunications will monitor closely the technological developments in this field in greater detail in order to ensure the respect for data protection and privacy in the context of "ubiquitous computing".

Explanatory Note:

Radio-frequency identification tags (RFID tags) are currently being tested and increasingly being used as a more advanced form and possible replacement of bar codes ("smart labels"). The size of these microchips is about 1/3 of a millimetre (and smaller – "smart dust"). Most of them operate as passive transponders (without batteries) by listening to radio signals sent by transceivers (RFID readers) and using the energy of the received radio signal to reflect and answer it. Active RFIDs have a greater range (depending on the readers used). Since prices for RFID microchips and readers are dropping their widespread deployment becomes increasingly economically viable. RFID tags are likely to become essential drivers of ubiquitous (or pervasive) computing. Due to their storage and capacity for interactive communication they are far more powerful than bar codes. In addition they provide for unique identification of each tagged unit whereas bar codes are identical for every unit of the same product.

RFID tags can be used to install "smart shelves" in stores in order to better manage the supply chain and facilitate the replenishments of goods or supplies (e.g. the case of Gillette razors). They may also be used for easy (contact-less) payment at the point of sale especially if linked with credit cards. Furthermore an employer may use the technology to tag his property in order to reduce theft by employees. They could be linked with video surveillance cameras to check employee as well as customer behaviour. Specific documents may be tagged to be traced more easily in an office. Identity cards as well as travel documents (passports, visas) may be equipped with RFID tags. More recently the European Central Bank has announced that Euro notes will be issued with RFID tags in order to fight counterfeiting and money laundering as well as to control circulating notes. Washable RFID tags can be embedded in clothes ("wearable computing") in order to prevent or detect counterfeiting of specific brands and to prove the authentic manufacture of the product. Other possible applications range from car keys (immobilizers) to container management.

The RFID technology has numerous privacy implications. This is obvious in the case of implanted microchips But also in the more widespread case of tagged objects and goods undoubtedly the

information transmitted also refers to the person carrying or wearing (or otherwise associated with) a tagged item or a "constellation" of brands thereby revealing the individual's taste. Therefore personal data can be processed and transmitted or read with the help of RFIDs or at least such object-related information can easily be linked with personal information (e.g. when a credit card is used for buying the tagged item). RFID tags have the potential of tracking the movements of a person who possesses or handles tagged objects.

Plans to afford technical devices legal protection against circumvention may prevent data subjects from disabling or deactivating RFID tags which function in a privacy-unfriendly way (e.g. after having paid and left the shop).

Since this issue has led to a growing public debate in a number of countries it is recommended that the International Conference addresses the related privacy problems at this stage in order to encourage privacy-friendly solutions which have been proposed. The International Working Group on Data Protection in Telecommunications at its 34th meeting in Berlin on September 2 and 3, 2003, has expressed its support for this proposal.