THE IMPORTANCE OF INFORMATION SECURITY IN SAFEGUARDING HUMAN AND FUNDAMENTAL RIGHTS
CONTENT

• FOUR MASTERS
• PANTA REI
• LEGAL CULTURE
• INFORMATION SECURITY AS HUMAN RIGHT
• CLOSING COMMENTS
FOUR MASTERS

• James Purnell
• Zahir Sachak
• Daniel Harrington
• Ahti Saarenpää

WHAT IS CONNECTING THESE MASTERS?
James Purnell 'should face action' for leaving papers on train

James Purnell, the Work and Pensions Secretary, should face disciplinary action for leaving confidential Government papers on a train, a civil service union has suggested.

By James Kirkup, Political Correspondent
Last Updated: 6:53AM GMT 03 Nov 2008

Papers lost by James Purnell relating to a member of his constituency were later returned by his fellow train passengers Photo: EDDIE MULHOLLAND

The First Division Association, which represents Whitehall mandarins, said the minister should be treated in the same way as officials who mislay sensitive information
The Whitehall secrets were clearly visible to other passengers on the packed train

By the time the train reached Basingstoke, where Ms Gledhill got off, she had read:

- A document from Patrick Crawford, chief executive of the Export Credits Guarantee Department, which was marked 'Restricted' on every page and referred to negotiations within the Treasury over the supply of loans to the Airbus consortium at below market rates of interest to match US support for Boeing. Such information could potentially influence share prices.
- An embarrassing email in the Mandarins folder about a Talent Man trial
Tax website shut down as memory stick with secret personal data of 12million is found in a pub car park

By DANIEL BOFFEY
Last updated at 3:05 PM on 02nd November 2009

Ministers have been forced to order an emergency shutdown of a key Government computer system to protect millions of people's private details.

The action was taken after a memory stick was found in a pub car park containing confidential passcodes to the online Government Gateway system, which covers everything from tax returns to parking tickets.

An urgent investigation is now under way into how the stick, belonging to the company which runs the flagship system, came to be lost.
Ahti Saarenpää

- As expert evaluating the legal regulation of basic registers
- Suggesting legislation introducing restrictions on the use of information tools
- Gave the report out in September 2008

has left memory stick in ministry
CONTENT

• FOUR MASTERS
• PANTA REI
• LEGAL CULTURE
• INFORMATION SECURITY AS HUMAN RIGHT
• CLOSING COMMENTS
ADMINISTRATIVE STATE

INFORMATION SOCIETY  GENERAL JURISDICTION
CONSTITUTIONAL STATE

NETWORK SOCIETY

SPECIAL JURISDICTION
CONTENT

• FOUR MASTERS
• PANTA REI
• LEGAL CULTURE
• INFORMATION SECURITY AS HUMAN RIGHT
• CLOSING COMMENTS
LEGAL CULTURE (Modeér)

- LEADING LEGAL IDEAS
- CONTENT OF CONSTITUTIONS
- QUALITY AND TYPE OF NORMS
- PROCEDURAL TOOLS TO SOLVE CONFLICTS
- LAWYERS INFRASTRUCTURES
LEGAL TURBULENS?

Mario Losano
The information superhighway is a metaphor familiar from the Information Society. Information networks have become the new information superhighway. The same image is more than applicable in describing the constitutional state. We are fully justified in speaking of a legal superhighway that should provide the most direct route from human and fundamental rights to the interpretation of individual provisions in the law.
A democratic society and constitutional state that rely on information networks can be built only if accompanied by appropriate information security that can ensure the smooth functioning of the infrastructure and its use and provide legal protection for information throughout its lifespan.
CONTENT

• FOUR MASTERS
• PANTA REI
• LEGAL CULTURE
• INFORMATION SECURITY AS HUMAN RIGHT
• CLOSING COMMENTS
Stenograph writers maximize efficiency and productivity.
One of the new basic legal concepts is *information security*. It is an addition to the “family” of securities, one that has even prompted a reaction or two among lawyers. In Finnish legislation information security has even been defined: "Information security means the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data systems can be used by those who are entitled to use them. This definition in the Act on the Protection of Privacy in Electronic Communications falls short of the mark. It is lacking one essential element – law. The legislators have forgotten themselves."
• Recognizing and acting on the need for a wholly new body of legislation involves rather a lot of effort. We are even slower to notice changes in legal principles and slower still to detect changes in our legal culture. The philosophy of knowledge teaches us that knowledge resides in structures, and that structures change slowly. The legal culture in its different forms is no doubt a premier example of this.
In the realm of professional expertise, an understanding of information security has been and continues to be a no man’s land. It has never been recognized as part of the legal culture; responsibility for it has been left to professionals in administration and IT. For them the issue has until very recently been a new one and one of relatively minor importance.
LEGAL INFORMATION SECURITY

• In the long, long history of security, and its still brief electronic counterpart, the legal aspects have been neglected or dealt with through haphazard legislative measures.

• I have elsewhere described the progress in noticing this situation as a development characterized in the early 1990s by the attitude that data and information securities were as “nice thing to have“.

• It is possible to go beyond this – and we have – to an assessment of data security from the legal perspective as well.
LEGAL INFORMATION SECURITY

• In this perspective, in Finnish Legal Informatics we have pointed out that our right to data security is or should be a kind of *meta-level fundamental right*.

• It is a precondition for the proper realization of our other fundamental rights especially in e-government.

• The information superhighway should be secure, which is not the case to day.

• If this perspective is neglected, we will abandon the constitutional state and – when thinking e-government - revert to the administrative state.
FROM TECHNICAL TOOL
TOWARDS LEGAL VALUE
THREE PRACTICAL EXAMPLES

• COPLAND
• I v. FINLAND
• JYVÄSKYLÄ TAX OFFICE
CONSEIL DE L’EUROPE

COUNCIL OF EUROPE

COUR EUROPÉENNE DES DROITS DE L’HOMME
EUROPEAN COURT OF HUMAN RIGHTS
10. During her employment, the applicant's telephone, e-mail and internet usage were subjected to monitoring at the DP's instigation. According to the Government, this monitoring took place in order to ascertain whether the applicant was making excessive use of College facilities for personal purposes. The Government stated that the monitoring of telephone usage consisted of analysis of the college telephone bills showing telephone numbers called, the dates and times of the calls and their length and cost.
The applicant also believed that there had been detailed and comprehensive logging of the length of calls, the number of calls received and made and the telephone numbers of individuals calling her. She stated that on at least one occasion the DP became aware of the name of an individual with whom she had exchanged incoming and outgoing telephone calls. The Government submitted that the monitoring of telephone usage took place for a few months up to about 22 November 1999. The applicant contended that her telephone usage was monitored over a period of about 18 months until November 1999.
11. The applicant's internet usage was also monitored by the DP. The Government accepted that this monitoring took the form of analysing the web sites visited, the times and dates of the visits to the web sites and their duration and that this monitoring took place from October to November 1999. The applicant did not comment on the manner in which her internet usage was monitored but submitted that it took place over a much longer period of time than the Government admit............
In the case of I v. Finland,

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

Nicolas Bratza, President,
Lech Garlicki,
Ljiljana Mijović,
David Thór Björgvinsson,
Ján Šikuta,
Päivi Hirvelä,
Mihai Poalelungi, judges,
and Lawrence Early, Section Registrar,

Having deliberated in private on 24 June 2008,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 20511/03) against the Republic of Finland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Finnish national ("the applicant") on 20 June 2003. The President of the Chamber acceded to the applicant's request not to have her name disclosed (Rule 47 § 3 of the Rules of Court).

2. The applicant was represented by Mr S. Heikinheimo, a lawyer
44. The Court notes that the applicant lost her civil action because she was unable to prove on the facts a causal connection between the deficiencies in the access security rules and the dissemination of information about her medical condition. However, to place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the hospital’s record keeping at the material time. It is plain that had the hospital provided a greater control over access to health records by restricting access to health professionals directly involved in the applicant’s treatment or by maintaining a log of all persons who had accessed the applicant’s medical file, the applicant would have been placed in a less disadvantaged position before the domestic courts. For the Court, what is decisive is that the records system in place in the hospital was clearly not in accordance with the legal requirements contained in section 26 of the Personal Files Act, a fact that was not given due weight by the domestic courts.

**Law courts in Finland did not know personal data rules at all**
45. The Government have not explained why the guarantees provided by the domestic law were not observed in the instant hospital. The Court notes that it was only in 1992, following the applicant’s suspicions about an information leak, that only the treating clinic’s personnel had access to her medical records. The Court also observes that it was only after the applicant’s complaint to the County Administrative Board that a retrospective control of data access was established (see paragraph 11 above).

46. Consequently, the applicant’s argument that her medical data were not adequately secured against unauthorised access at the material time must be upheld.

**INFORMATION SECURITY AS HUMAN RIGHT?**
46. Consequently, the applicant’s argument that her medical data were not adequately secured against unauthorised access at the material time must be upheld.

47. The Court notes that the mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place. Such protection was not given here.

48. The Court cannot but conclude that at the relevant time the State failed in its positive obligation under Article 8 § 1 of the Convention to ensure respect for the applicant’s private life.

49. There has therefore been a violation of Article 8 of the Convention.
Luvaton tiedonhaku toi sakkoja verovirkailijalle

Julkaisu: 15:06

STT

JYVÄSKYLÄ. Verovirkailija sai sakkoja katseltuaan luvattomasti neljän tuttavansa henkilötietoa. Jyväskylän käräjäoikeus tuomitsi hänet tiistaina verkavelvollisuuden rikkomisesta ja henkilörekisteririkoksesta.

Sisä-Suomen verovirastossa työskentelevä nainen oli katsellut neljän henkilön tietoa verohallinnon tietojärjestelmästä, vaikka ne eivät liittyneet hänen virkatehtäviinsä. Hän myönsi katselleensa tietoa yksityiselämäänsä liittyvistä syistä.

INFORMATION SECURITY IS A PART OF MANAGEMENT
Lex Nokia” gets blessing from Constitutional Law Committee

According to a statement issued by Parliament's Constitutional Law Committee, an amendment to the Act on Data Protection of Electronic Communications may be passed through the normal legislative process.

The so-called ”Lex Nokia” - also known as the ”snooping law” - would allow employers to investigate the log data of employees’ e-mails, if the company has reason to suspect that corporate secrets are leaking out of the company or that the employer’s communication networks are being misused.

However, the employer would not be allowed to look into the content of the messages themselves, but only to examine the e-mail log including the information on the senders, the recipients, and the size of employee messages as well as the volume of traffic and other matters relating to the company's e-mail usage.

Hence the new law would not be in violation of the Act on Protection of Privacy in working life, which stipulates that the employer must not endanger the secrecy of private and confidential messages, said the Constitutional Law Committee, chaired by Kari Nokko (National Coalition Party).

However, the Committee stressed that the employer can only investigate the e-mail log only after it has taken all other necessary steps to prevent possible wrongdoings.

This requirement is stipulated by law. The employer would nevertheless wanted to emphasise that such measures take priority over any other course of action.

The Committee noted further that log data on e-mail messages can be monitored only after it has become evident that there is no other way to investigate a suspected leak of corporate secrets.
I was among the experts who opposed the bill to amend the Act. My statement ended with the following words:” It must also be pointed out that modern IT offers effective information security solutions for managing trade secrets. The requirement that a restriction of fundamental rights should be essential is thus not, in my view, met in the present case. Poor business management that overlooks opportunities to use sophisticated forms information security should not be an adequate reason for restricting the fundamental rights of individuals in working life”. 
I was among the experts who opposed the bill to amend the Act. My statement ended with the following words:” It must also be pointed out that modern IT offers effective information security solutions for managing trade secrets. The requirement that a restriction of fundamental rights should be essential is thus not, in my view, met in the present case. Poor business management that overlooks opportunities to use sophisticated forms information security should not be an adequate reason for restricting the fundamental rights of individuals in working life”. 
CONTENT

• FOUR MASTERS
• PANTA REI
• LEGAL CULTURE
• INFORMATION SECURITY AS HUMAN RIGHT
• CLOSING COMMENTS
In my report, I proposed that Finland should enact a law on data stores that would govern basic registers as well as a general law on information security. In addition, I suggest legislation introducing restrictions on the use of information tools. These three laws would furnish a basis for a new information security culture that would take its place as a part of democracy and the legal culture.
• This significant change in the legal culture of the constitutional state unequivocally requires that information security should be included among our fundamental rights. It is an element of the essential social contract that underpins the Network Society. Accordingly, in my report I have proposed that information security be expressly included among the values protected by the Constitution. This is perhaps a fitting way to conclude a presentation on the importance of information security in the constitutional state.
“Strong data protection rules are needed to prevent the emergence of a surveillance society”

[26/05/08] Surveillance technology is developing with breath-taking speed. This creates new instruments in the struggle against terrorism and organised crime, but also raises fundamental questions on the right to privacy for everyone. Individuals should be protected from intrusions into their private life and from the improper collecting, storing, sharing and use of data about them. Terrorism and organised crime must be combated - but not with means which undermine basic human rights.

Nowadays there are technologies to monitor, screen and analyse billions of telephone and email communications simultaneously; to use virtually undetectable listening and tracking devices; and to install ‘spyware’ surreptitiously on someone’s computer which can secretly monitor the online activities and emails of the user and even turn on the computer’s camera and microphone.

It is sometimes said that only those who have something to hide should be fearful about these new measures. However, the notion that if you have nothing to hide you have nothing to fear puts the onus in the wrong place – it should be for States to justify precisely the interferences they seek to make on privacy rights, not for individuals to justify their concern about interferences with their basic human rights.

The use of such new facilities and expanded competencies for the police and security services requires enhanced democratic and judicial control.

Already, the storing of enormous amounts of personal data in social security-, medical- and police databases(1) is a matter of concern. The recent loss, in the United Kingdom, of a database containing personal data on 25 million people serves as a stark reminder of the risks.

The Commissioner for Human Rights has released a compendium with the 27 viewpoints written during his second year in office. This free publication is available in English, French and Russian.

To order

- “Time to recognise that human rights principles apply also to sexual orientation and gender identity” (14/05/08)
- “Aged people are too often ignored and denied their full human rights” (28/04/08)
- “International human rights bodies worldwide need more support and more self-criticism” (14/04/08)
- “The key to the promotion of Roma rights: early and inclusive education” (31/03/08)
- “States should not impose penalties on arriving asylum-seekers” (17/03/08)
THE END