Data Protection: Assessing Good Practice

Alvin West

Audit Team Manager

Information Commissioner's Office

30th Sept 2011

What is good practice?

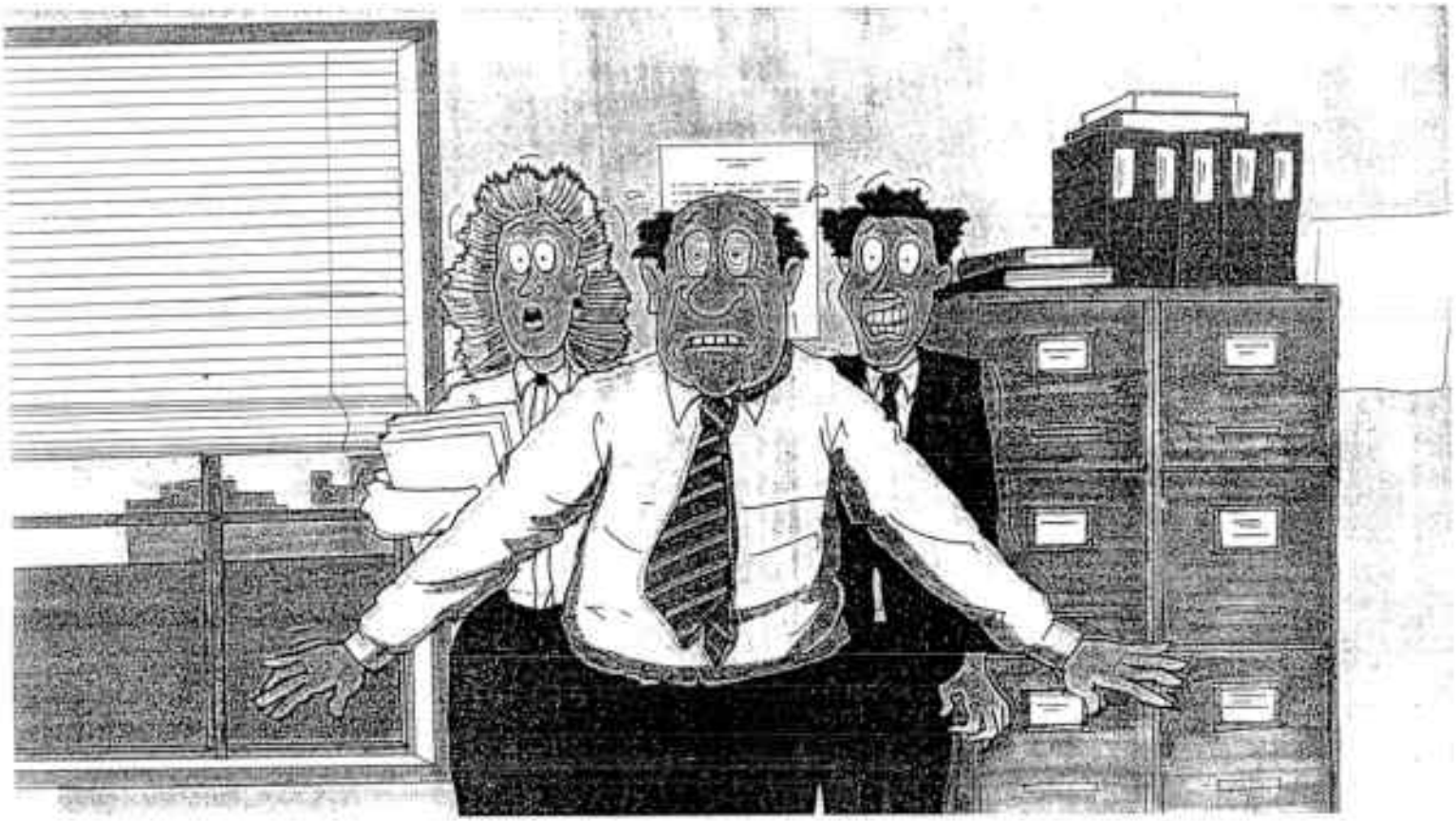
- What does the DPA say?
  - Good practice is defined as such practice for processing personal data as appears to be desirable. Includes, but is not limited to, compliance with the requirements of the act
- What does this mean in practice?
  - Efficient, effective, robust policies and procedures exist and are working in practice to ensure information is handled correctly and the organisation is aware of, and fulfilling, its obligations

ico.

Good Practice Audit

- Seen as being key to educating and assisting organisations to meet their obligations
- Use audit, assessment and practical advice and recommendations to improve the way organisations deal with information rights issues
- Assist the ICO to share knowledge and promote good data protection practice through publishing audit outcomes
- Allow organisations to show their commitment to, and recognition of, the importance of data protection
- Risk based approach

ico.



ico.

ico.

How?

Assessment Notices

Consensual Audit

Short Audit

Undertakings

Self assessment questionnaires

Self Audit

Audits: consensual and compulsory

- So far, all of our audits have been consensual – i.e. scope and time agreed with the data controller or point of contact
- Consensual audits review the control framework for complying with the Data Protection Act, ICO codes of practice and guidance
- Now have powers to conduct a 'compulsory' audit following the issue of an Assessment Notice.

ico.

Assessment notices

- Under section 41A of the DPA the Commissioner may serve certain data controllers with a notice ('Assessment Notice') imposing specific requirements of the data controller

- Used in circumstances where there is a risk that individuals' data will be compromised but the organisation is unwilling, for whatever reason, to engage constructively with ICO

- The assessment notice is for the purpose of enabling the Commissioner to determine whether the data controller has complied or is complying with the principles

Our audit approach – overview

- Agree a scope of work with the organisation
- Carry out an off-site check of an organisation's documented policies and procedures
- Carry out an on-site review of the procedures in practice for processing personal data
- Provide a report with recommendations
- Write an executive summary that we can publish on our website, with the consent of the organisation
- Carry out a follow-up review – dependent upon the outcome of the original audit

ico.

Key scope areas

- Governance
- Training and awareness
- Records management
- Security
- Requests for personal data

What type of things do you think we would be looking for in these areas?

ico.

Governance

Policies and procedures

- Making sure policies cover all aspects of DPA not just SARs and security
- Ensuring policies are dated and version controlled and available in one location
- Communication of policies

Governance structures

- Ensuring someone at a senior level has ownership of data protection matters and that role is clear to others in the organisation

ico.

Governance (contd)

Measures

- Management information including more than just performance against the 40 day deadline

Audits

- Role of internal audit, spot checks and routine monitoring of compliance

Returns

- Explicitly referring to information governance issues in publicly available documents
- Risk registers

Risk assessments

- Privacy impact assessments

Training & awareness

Induction

- Making sure permanent, temporary, contract and third party staff are aware of policies

Role based training

Refresher training

E learning

- Maintaining records to identify gaps

IT access

- Ease of access to information
- Access to personal data after data protection training

ico.

Records management

Owner

Inventory of personal data/audit of corporate information assets

Consistent application to manual and electronic records

Fair processing

Tracking of manual records/home working

Retention

Disposal

ico.

Security

IT

Information Security Framework including Policy and Controls

Asset Management – fixed and mobile media including laptops, memory sticks, decommissioning etc

Incident Management

Training

Identity Access Management – joiners, leavers, movers, regular review
third party contractors

Network Access Controls – firewalls, anti-virus updates, encryption

Remote Working

Web application and Cloud computing

ico.

Security

Physical

Location of documents/servers – third party contractors

Security of buildings/cabinets etc.

Key control

Access control

Confidential Waste

ico.

Requests for personal data

Procedures
- Retrieval process from all 'likely' sources of personal data
- Responsibilities in job descriptions for processing SARs
- Reporting performance
- Complaints handling

Monitoring
- SARs logs
- Application of Redactions and Exemptions
- Disclosures procedures

Data sharing
- Ownership
- Use of data sharing protocols/ updating
- Records of data sharing

ico.


HAPPINESS IS
A COMPLETED
AUDIT
AUDITOR

ICO audit activity

- Growing number of audits
- Growing team
- More diversity of organisations audited
- Greater sharing of outcomes and good practice

ico.

Questions?

The Information Commissioner:

Data Protection - the ICO Penalty Regime. (And how to avoid it!)

Richard Kerr
Enforcement Team Manager.

21st September 2011

Information Commissioner's Office

Two important questions!

1. **Are you a data controller?**
   You will know the many changes adopted in reorganising barrister's chambers in recent years. These are one of the many reasons most barrister's are now considered to be data controllers in their own right, and hence must notify as such.

   If at all unsure you must check your status.

2. **Does your Bar Mutual policy cover you for actions attracting an ICO CMP?**

ico.
Information Commissioner's Office

THE INDEPENDENT

Lost in the post: the personal details of 25 million people

The Daily Telegraph

Now data on all prisoners is lost

By Robert Winnett
Deputy Political Editor

THE Home Office has lost confidential information on every prisoner in the country and more than 10,000 serious criminals causing yet another government data crisis.

It has led to fears that the taxpayer may now face a multi-million pound compensation bill from criminals whose safety may be compromised.

The latest addresses of some of Britain's most prolific and serious offenders – including those who have committed violent and sexual crimes – are understood to be among the data missing.

They were on a computer memory stick used by Home Office consultants that has gone missing over the past week. An investigation was started yesterday and the police have been informed.

Home Office officials are in discussions with the Information Commissioner about what steps need to be taken to protect those whose privacy has been jeopardised.

The Commissioner said last night that "sounding questions must be answered"

Continued on Page 2

Mail Online

Home Office censured over loss of memory stick containing information on 84,000 prisoners

THE Sun

DATA ON 84,000 PRISONERS LOST

Now lags could sue over latest ID blunder

DAILY Mirror

BENEFITS DISASTER

MISSING: Names, addresses, dates of birth, NI numbers and bank details of 25m people

CHECK YOUR ACCOUNTS

Informal Resolution

By far the majority of our breaches are dealt with by finding a mutually agreeable 'Informal Resolution' with the DC.

As the title states, this is INFORMAL regulatory action and permits room for common sense in the lesser, every day cases.

Informal Resolutions are completed simply by the exchange of letters, although we are always happy to speak with you on the telephone.

ico.

Thematic Inspection (Walk through)

Further informal action, conducted in agreement with the DC.

May be resolution on it's own or may be part of any other regulatory action.

Does NOT amount to an audit, but like an audit we are unlikely to pursue any other matters discovered in the course of such action.

ico.

Undertakings.

Undertakings are again an INFORMAL procedure NOT catered for within the DPA 1998.

In exchange for the Commissioner not exercising his powers under section 40 of the Act (Enf. Notice) the DC enters into a written undertaking to complete an agreed course of remedial action. The Undertaking is published on the ICO web site and may be accompanied by a press release.

Undertakings can be agreed simply by exchanging correspondence, or the Case Officer may wish to visit the breach site.

ico.

Enforcement Notice

- Formal regulatory power under S40 DPA 1998.
- If the Commissioner is satisfied that a data controller has contravened or is contravening any of the DP principles (and damage or distress has, or is likely to, result) Commissioner may serve him a notice requiring him to....
- take (or refrain from taking) such steps as are specified within the notice. OR

ico.

Enforcement Notice

- refrain from processing any personal data (or to refrain from processing PD for a purpose specified within the notice) – after such time as specified.
- In deciding whether to serve an enforcement notice, the Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.
- Breach of an Enforcement Notice is a Criminal Offence.
  Summary conviction = fine not exd. £5,000.
  On indictment = Unlimited fine.

ico.

Civil Monetary Penalties. (Origins)

- Continued significant losses of personal data.
- Previous powers deemed inadequate.
- Public calls for criminal offence.
- Preferred option was power to impose a Monetary Penalty – civil sanction.
- New power inserted into section 55 of Data Protection Act 1998 by section 144 of the Criminal Justice and Immigration Act 2008 (CJIA).

ico.

Civil Monetary Penalties (Origins 2.)

- Enhanced power for ICO to impose monetary penalties.
- Sanction and a deterrent to data controllers who may otherwise ignore their responsibilities under the Data Protection Act.
- Encourage data controllers to approach ICO and promote compliance.
- Improve public confidence.

ico.

Main features

- ICO may serve a Monetary Penalty Notice on a data controller requiring payment of a Monetary Penalty which must not exceed £500,000 (20% discount!)
- Applies to all data controllers in the private, public and voluntary sectors except Crown Estate Commissioners or a person who is a data controller by virtue of section 63(3) DPA 1998-Royal Household

ico.

FAX Machines!!

=

ico.

Hertfordshire County Council – Overview – June 2010.

- Papers concerning a live court case involving detailed allegations of the abuse of a child by a relative, requested by a barrister at court, were faxed to a member of the public in error.
- Very similar matter repeated 13 days later.
- CMP £100,000

ico.

Barristers - antecedents!

Prosecution case file left unattended for 4 minutes in Crown Court. Picked up and part read by one of the defendants. SPD ++.

Full case file in care proceedings left in foot well of car overnight in supermarket carrier bag. Car broken into and file stolen. SPD +++

Unencrypted laptop, containing copious case notes, stolen by means of domestic burglary. No physical security. SPD ++

Judge leaves unencrypted laptop on train. SPD ++

Barrister gets puncture in car tyre and changes wheel at roadside. Cleans hands on case file papers and places in nearby public street waste bin. SPD +

ico.

How to avoid a data breach.

- Treat each of your case files, or your laptop, as though they were £10,000 in cash! £££££££££££££££££££££!
- Always ensure your electronic PD is encryption & password protected. (Then you don't need to inform us!!)
- Never leave PD in an unattended car.
- Never leave PD unattended in any building unless it is **secure**. Agree who in the office is charged with it's care.
  (I do appreciate that you have to do the day job!)
- Remember that your phone is likely to contain a considerable volume of PD / SPD. (Email attachments etc.)

ico.

How to avoid a data breach 2.

Never fax PD unless absolutely necessary, then you must use 'Ring ahead' / safe haven.

When travelling set a reminder on your phone / watch etc. to ensure that you have collected all your papers / data just prior to the arrival of your transport at your destination!

If you incur a breach do all you can to recover the situation. The ICO can advise on whether you need to report it to our office and, if so, how to do so. (**Your actions post breach are important!**)

Keep an absolute minimum of data at your home for the minimum of time. (i.e. None when you are on holiday!)

ico.

Data Protection/the ICO Penalty Regime.

Any questions?

ico.

Freedom of information and research data

Victoria Cetinkaya, Senior Policy Officer, Information Commissioner's Office

13 September 2011

The Information Commissioner's Office

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

ico.

ICO's role

Enforce and regulate
- Freedom of Information Act
- Data Protection Act
- Environmental Information Regulations
- Privacy and Electronic Communications Regulations

Provide information to individuals and organisations

Adjudicate on complaints

Promote good practice

ico.

Our performance – 2010/11

c 206,585 – calls to our helpline
c 2.4m – visits to our website

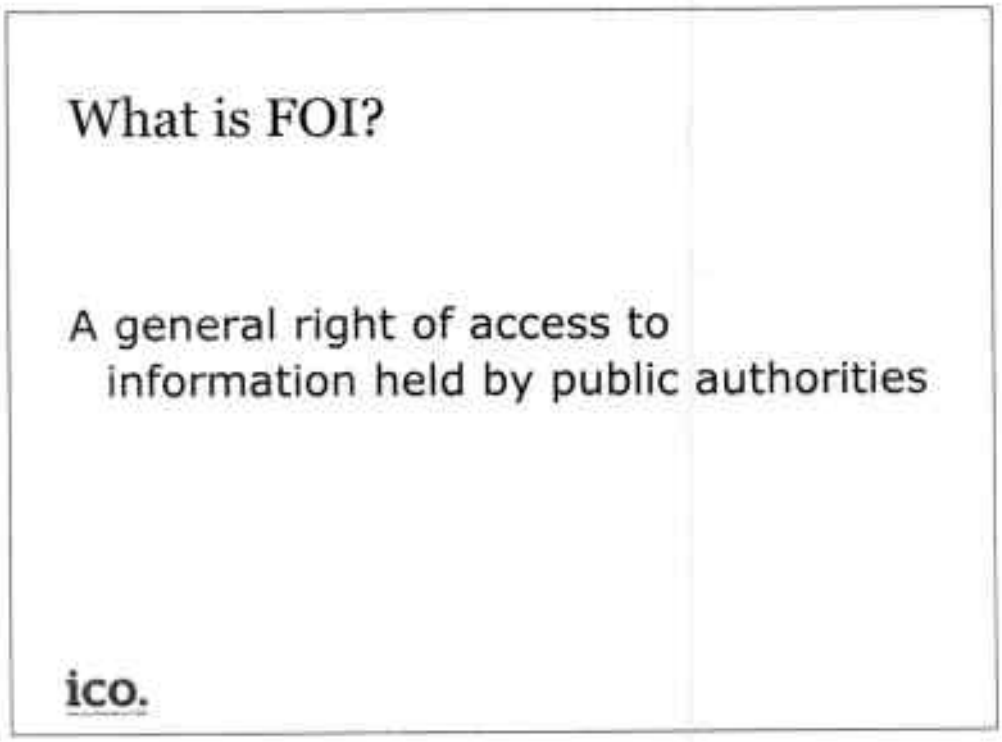
Data protection

- 26,227 – data protection cases received
- 29,685 – data protection cases closed
- c 339,298 – organisations notifying

Freedom of information

- 4,374 – freedom of information cases received
- 4,369 – freedom of information cases closed

ico.



- accountability and transparency
- spending of public money

NB – it is access to the public at large, not just an individual.

Also note that reference to 'FOI' in general terms here includes the Environmental Information Regulations, which are very similar.

Important parts of the FOIA

- Section 8 – valid request
- Section 10 – time for compliance
- Section 12 – cost limits
- Section 14 – vexatious / repeated requests
- Section 16 – duty to provide advice and assistance
- Section 17 – refusal of a request
- Section 19 – publication schemes

ico.

Section 8

In writing (email OK). Include name, address for correspondence. Twitter OK.

Section 10

20 working days to reply. Clock stops if need further info, perhaps to narrow down the request

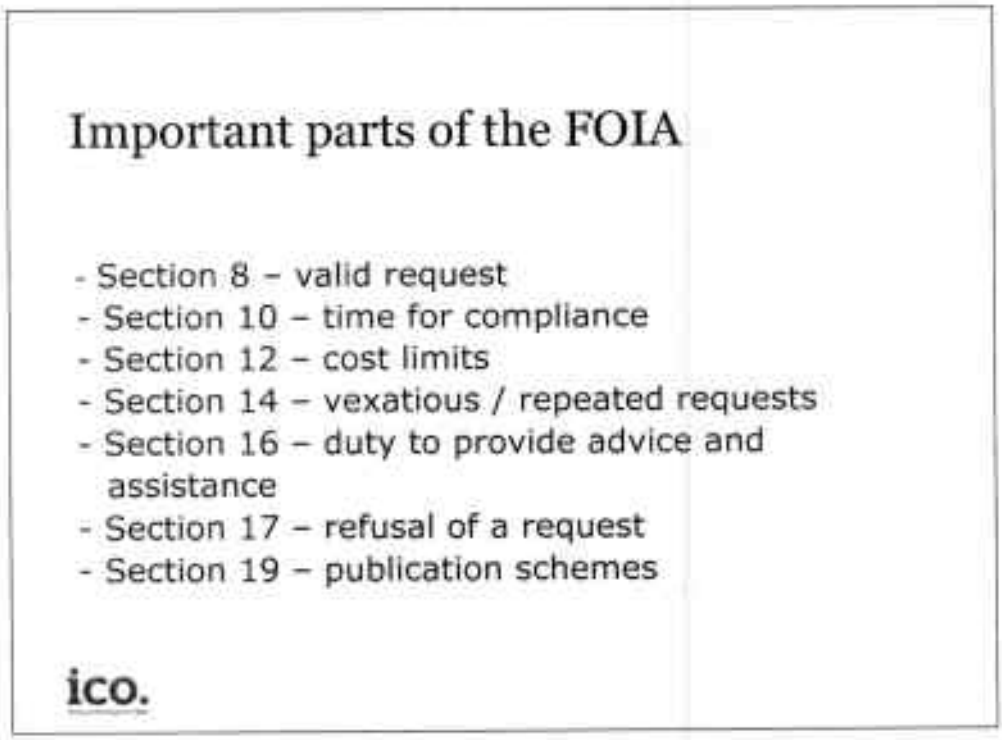
Section 12

Costs - £450.00 max charged at £25.00 per hour. NOT the costs of locating or redacting the information. Includes cost of printing, paper etc. If exceed, speak to applicant to try to narrow the request to bring it within cost limits.

Section 14

Vexatious requests, not requestors. Consider:

- fairly seen as obsessive?
- harassing the authority or causing distress to staff?
- compliance impose a significant burden re expense / distraction?
- designed to cause disruption or annoyance?
- lack any serious purpose / value?



Section 16

Duty to provide advice and assistance. Se s45 CoP (MoJ)

Section 17

Refusal notice – issue asap and always within 20 working days.

Clear, specific. Why info is being withheld.

Section 19

Publication schemes – proactive release of information.

Adopt the ICO model scheme and routinely disclose. If get a request, can refer to publication scheme.

ICO going to start work on updating the HE publication scheme definition document in conjunction with the HESP.

Link with RCUK Common Principles on Data Policy and guidance on data management plans.

The exemptions

- Over 20 in total
- Tightly drawn up; their use is limited
- Presumption of disclosure
- Cover areas such as:
  - National security; defence
  - Law enforcement; court records
  - Parliamentary privilege
  - Formulation of government policy
  - Legal professional privilege
- The public interest test

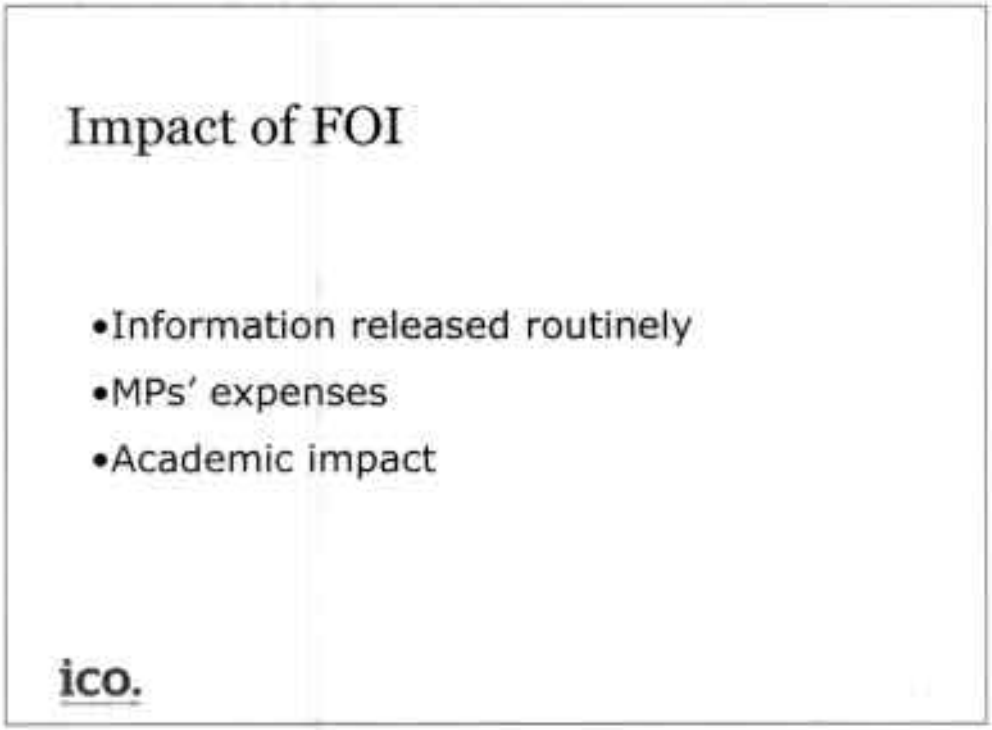
ico.

Some exemptions are absolute; some are qualified and require a further public interest test – e.g. LPP can be overridden if it is in the public interest to disclose, especially if advice old and the issue no longer 'live'.

Exemptions especially relevant to HE and research

- Information accessible by other means
- Information intended for future publication
- International relations
- Prejudice to effective conduct of public affairs
- Personal information
- Information provided in confidence
- Commercial interests

ico.



Routine release is now common – e.g. salaries and expenses of CEOs of local authorities, or chief police officers

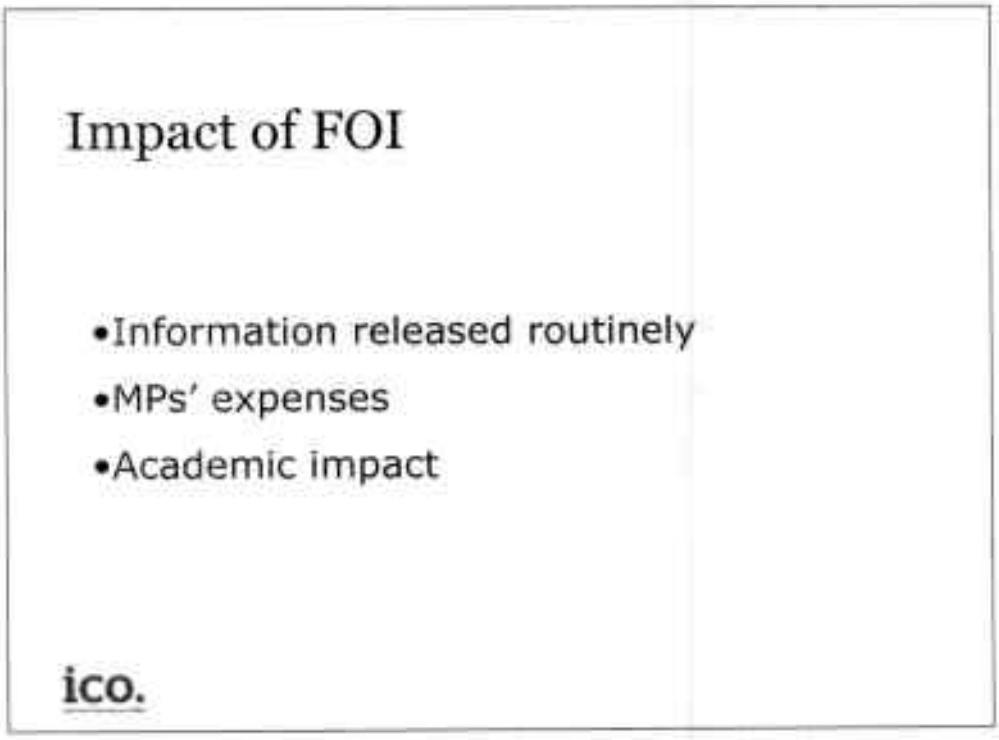
MPs – use of FOI showed a corrupt process, and that some MPs were abusing it. Resulted in prison sentences for a few.

Academic impact – UEA / QUB / UCLAN

UEA

The complainant made a number of requests for information related to the involvement of some of UEA's staff in the Intergovernmental Panel on Climate Change. The Commissioner has found that the public authority breached regulation 14(2) of the EIR by failing to provide a response to a request within 20 working days and breached regulation 5(2) by failing to provide a response to other requests.

(UEA tried to rely on exemptions within the FOIA (s12 cost limits, s27 international relations, s36 prejudice to effective conduct of public affairs, s41 info provided in confidence) but the information was in fact environmental as defined in the EIRs and therefore had to be dealt with under the EIRs).



QUB

The complainant requested electronic data relating to tree ring research (dendrochronology). QUB confirmed that it held the requested information but refused to provide it citing section 12 of the Act. The Commissioner indicated to the public authority that the withheld information fell within the definition of environmental information under the EIR. The public authority subsequently cited the exceptions at regulations 12(4)(d), 12(4)(b), 12(5)(c) and 12(5)(e) to refuse the information. The Commissioner finds that none of the exceptions is engaged and the withheld information should therefore be disclosed. The Commissioner also recorded a number of procedural breaches in the public authority's handling of the request.

QUB argued that the requested information should be withheld under the following exceptions:

- Regulation 12(4)(d) – information that is unfinished or in the course of completion, - But ICO said that the data is not unfinished or incomplete, rather that, whilst the research utilising this data is ongoing i.e. the analysis of the data, the data itself has already been collected and is therefore not unfinished or incomplete.

Impact of FOI

- Information released routinely
- MPs' expenses
- Academic impact

ico.

• Regulation 12(5)(c) – intellectual property rights – but ICO said that in order to engage the exception, it is necessary to demonstrate that QUB hold intellectual property rights in respect of the raw tree ring data and that an adverse effect to those rights would arise as a result of disclosure of that data. The ICO was not persuaded that QUB does in fact hold intellectual property rights in relation to the withheld information. Whilst the research that was undertaken and published by QUB using the data as a tool might well attract intellectual property rights, it is unclear to the Commissioner as to how the raw tree ring measurement data itself could attract such rights. No clear argument received.

• Regulation 12(5)(e) – commercially confidential information – but QUB collected the data itself, so it does not attract a duty of confidence provided by law as it is primary information generated by QUB itself and not shared with a third party. The information does not have the quality of confidence.

regulation 12(4)(b) on the grounds that the request was manifestly unreasonable (time taken to extract, copy, collate and prepare info for release).

QUB also said the info would be meaningless for the complainant in its current format – but ICO said there is no requirement for applicants to demonstrate how they would use the info.

Impact of FOI

- Information released routinely
- MPs' expenses
- Academic impact

ico.

UCLAN

The complainant requested copies of the course materials issued to undergraduate students for the BSc (Hons) in Homeopathy. UCLAN withheld the requested information by virtue of the exemptions contained in sections 21, 43(2), 41, and 36(2)(c). The Commissioner found section 41 was engaged in respect of specific portions of the course materials but that none of the other exemptions were engaged, and ordered the disclosure of the requested information apart from the portions withheld under section 41. He also found the public authority in breach of sections 1(1)(b), 10(1), and 17(1). Information Tribunal appeal number EA/2009/0034 dismissed.

S21 - reasonably accessible by other means (pay fee, enrol on course) – ICO said fee for 3 years' tuition not reasonable in comparison with fees which may be charged by PAs for complying with FOI requests.

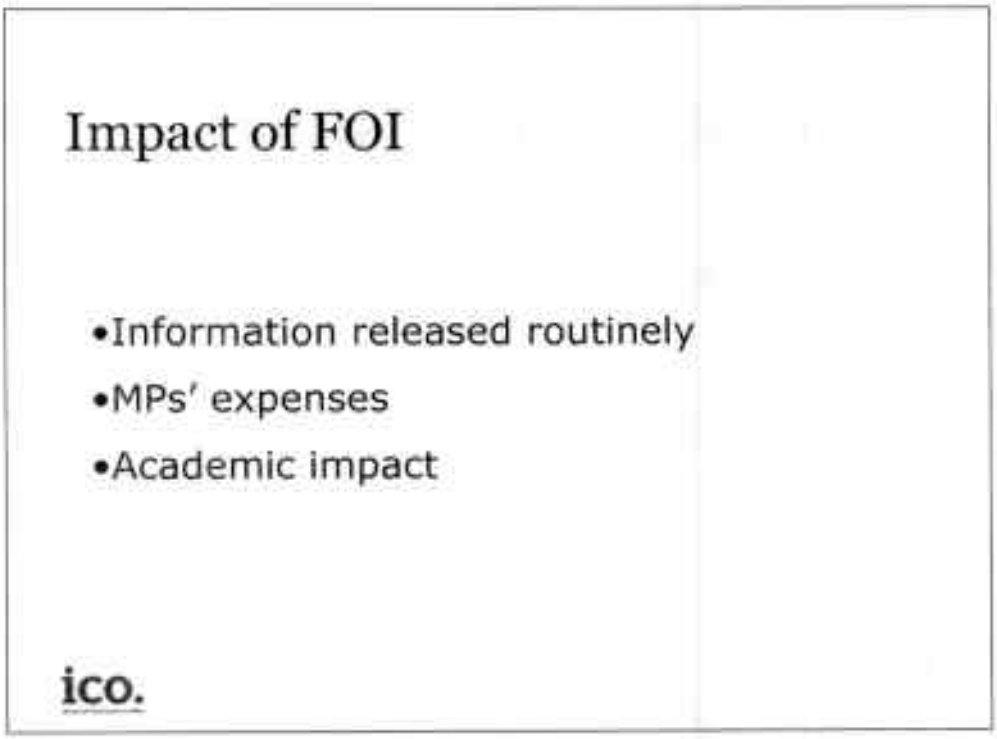
Impact of FOI

- Information released routinely
- MPs' expenses
- Academic impact

ico.

S43(2) – prejudice commercial interests (of UCLAN or 3rd party) – UCLAN concerned that private providers would use their course content, thus prejudicing UCLAN's position. The ICO found that section 43(2) was incorrectly engaged by virtue of the fact that the public authority's ability to recruit students is not a commercial interest within the contemplation of section 43(2). In addition to his finding on commercial interests the Commissioner finds that section 43(2) would in any case not be engaged as the likelihood of prejudice to the public authority's ability to recruit students as a result of disclosure under the Act is no more than the likelihood of prejudice resulting from the availability of the course materials to students already enrolled on the course.

S41 – information provided in confidence (case studies) – ICO found this was correctly applied



S36(2)(c) – prejudice the effective conduct of public affairs - The ICO recognises that if as a consequence of disclosure in this case, the public authority received a large number of requests for the course materials for all or most of its courses, it could be so disruptive that section 36(2)(c) might be engaged. However, he does not consider that it is at all plausible that this would happen, and that the public authority has not considered if there is any evidence in support of the likelihood that this would be the case. As already noted by the public authority, course materials which are available to students enrolled on a course are already at risk from further dissemination, and it is unlikely that disclosure in this case would lead to substantial applications for the course materials for the BSc in homeopathy or any other courses offered by the public authority in light of the fact that they are readily available to potentially thousands of students therefore making them quite easily accessible to anyone determined enough to have them. He does not accept that for the material other than the case studies a strong level of control exists, as argued by the public authority.

ICO work with the HE sector

- ICO higher education sector panel on FOI and DP

- Research subpanel

ico.

ICO Guidance for Higher Education: research information and the FOIA/EIRs

- due for publication September 2011
- to include guidance on:
    - future publication
    - commercial interests and IPR
    - academic discourse
    - peer review
    - international relations
    - personal information
    - vexatious requests

ico.

The work continues: publication schemes

- updating of publication scheme definition document for the HE sector

- proactive disclosure of research information

ico.

Subscribe to our e-newsletter
at www.ico.gov.uk

Follow us on Twitter
at www.twitter.com/iconews

ico.

Freedom of information and research data

Victoria Cetinkaya, Senior Policy Officer, Information Commissioner's Office

13 September 2011

The Information Commissioner's Office

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

ico.

ICO's role

Enforce and regulate

- Freedom of Information Act
- Data Protection Act
- Environmental Information Regulations
- Privacy and Electronic Communications Regulations

Provide information to individuals and organisations

Adjudicate on complaints

Promote good practice

ico.

Our performance – 2010/11

c 206,585 – calls to our helpline
c 2.4m – visits to our website

Data protection

- 26,227 – data protection cases received
- 29,685 – data protection cases closed
- c 339,298 – organisations notifying

Freedom of information

- 4,374 – freedom of information cases received
- 4,369 – freedom of information cases closed

ico.

What is FOI?

A general right of access to information held by public authorities

ico.

Important parts of the FOIA

- Section 8 – valid request
- Section 10 – time for compliance
- Section 12 – cost limits
- Section 14 – vexatious / repeated requests
- Section 16 – duty to provide advice and assistance
- Section 17 – refusal of a request
- Section 19 – publication schemes

ico.

The exemptions

- Over 20 in total
- Tightly drawn up; their use is limited
- Presumption of disclosure
- Cover areas such as:
  - National security; defence
  - Law enforcement; court records
  - Parliamentary privilege
  - Formulation of government policy
  - Legal professional privilege
- The public interest test

ico.

Exemptions especially relevant to HE and research

- Information accessible by other means
- Information intended for future publication
- International relations
- Prejudice to effective conduct of public affairs
- Personal information
- Information provided in confidence
- Commercial interests

ico.

Impact of FOI

- Information released routinely
- MPs' expenses
- Academic impact

ico.

ICO work with the HE sector

- ICO higher education sector panel on FOI and DP

- Research subpanel

ico.

ICO Guidance for Higher Education: research information and the FOIA/EIRs

- due for publication September 2011
- to include guidance on:
    - future publication
    - commercial interests and IPR
    - academic discourse
    - peer review
    - international relations
    - personal information
    - vexatious requests

ico.

The work continues: publication schemes

- updating of publication scheme definition document for the HE sector

- proactive disclosure of research information

ico.

Subscribe to our e-newsletter at www.ico.gov.uk

Follow us on Twitter at www.twitter.com/iconews

ico.

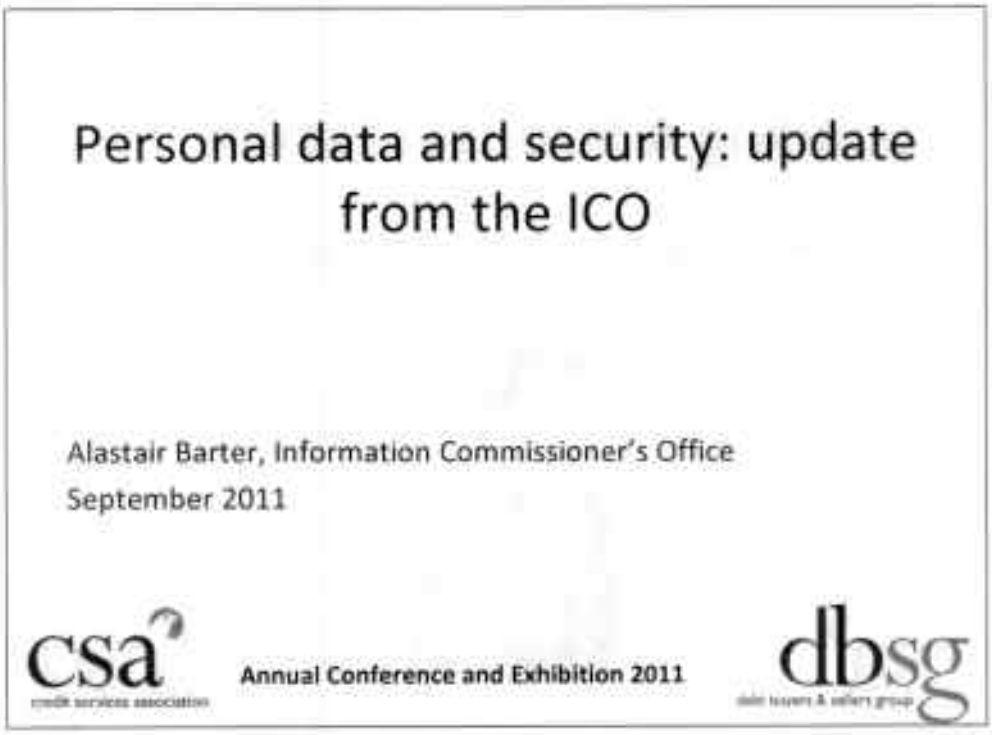
Building A Stronger Future

CSA and DBSG Annual Conference and Exhibition 2011

csa
credit services association

dbsg
debt buyers & sellers group

8th Sept 2011



Good afternoon and thank you to the organisers at the CSA for giving me the opportunity to speak to you today

I'm here to give an brief overview of data security from the point of view of the ICO – the data protection regulator

The ICO has an enforcement and advisory remit which assists us in upholding data protection law and offer guidance to data processors and data subjects.

Data security issues often make the headlines – lost laptops, stolen records, intrusive CCTV systems, hacked databases and identity theft – all generates interest. Why such human interest? Because it could happen to anyone – we could all be the data subject who's personal information has gone missing or the data controller who lost it.

Advancing technology has created seemingly infinite possibilities in the way data is collected, shared, stored, analysed, sold – the list goes on.

The pace of change has been so quick that it has become difficult to evaluate the true data protection risks of new technologies at the same pace as the technology is integrated into the way we live and work. Social networking, cloud computing, geolocation data, biometrics and facial recognition to name a few modern examples, all raise data protection issues.

In fact, the legislation itself is changing to reflect the fact that the way we process personal information today differs so much from that of the mid-1990's when the DPA was drafted. A key part of the review of the EU data protection directive is how the legislation can address the impact of new technologies

I'm going to focus on some of the data protection basics in terms of data security

Legal Requirements: What obligations does the DPA place on the data controller?

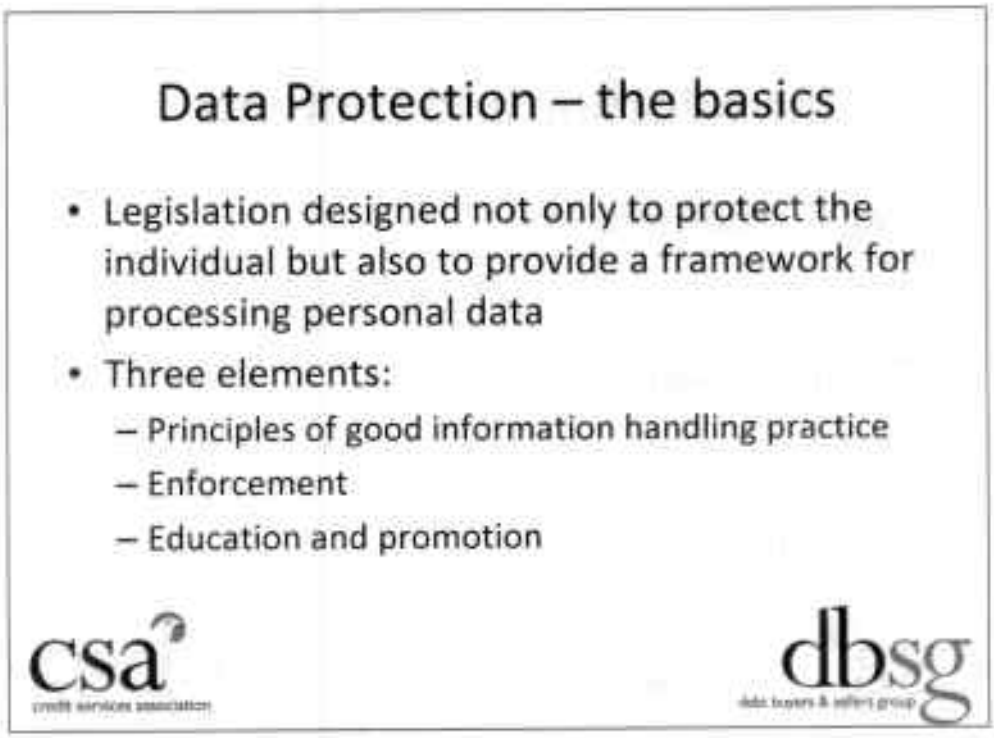
Legal Requirements: What rights does it provide to the data subject?

Penalties: What powers does the ICO have to penalise data controllers that do not adhere to the DPA?

Payment Cards: Recent stories have shown that protecting one element of personal data – payment card data – is important to avoid obvious consequences to those who have had their data lost and those who have compromised it

Risks: What risks does poor data governance and security pose to businesses?

Good Practice: Some advice on how DPA compliance can be achieved and a mention of the ICO audit function – a free service available to public and private sector organisations.



The DPA provides a framework based around 8 principles of information handling which, if followed correctly, should serve to protect the individual and help the data controller maintain compliance with the DPA

A main function of the legislation – and the ICO - is to promote these principles – the cornerstone of good data governance - through education and promotion of good practice

Achieved through Codes of practice which use real world examples to explain how the principles work in practice

guidance

helpline available to the businesses and the general public

liaison functions where the ICO engage with major stakeholders be they Government Departments or private sector Organisations

The legislation gives the ICO enforcement powers which allow the commissioner to fine organisations up to £500,000 for serious breaches of the DPA

Adopt a problem orientated approach – identifying issues that could bring with them DPA concerns and work to mitigate the risks before they become full-blown cases of data protection breaches. Not easy hence much work on Cloud computing, geolocation data, behavioural advertising and biometric/facial recognition

Brief look at those principles

Apologies to those of you that are well versed already

Each brings with it too much detail to cover in 25 mins or so

As long as you can justify processing personal data for a specific purpose

As long as you don't overdo the amount of data you record to achieve that purpose and what you do hold is accurate, up to date and disposed of when no longer required. If all rights of the data subject are understood as well as the restrictions surrounding disseminating it outside the EU – compliance can be achieved without being an onerous task.

As this is an update on data security I'd like to focus on the seventh DP principle - appropriate technical organisational measures being in place to secure the personal data

Oft-discussed topic as it is not within the legislation what constitutes 'appropriate measures'

Valuing data in monetary terms is perhaps something of a new concept

Everything else in business is assigned a monetary value – people, stock, property – so it would be strange to consider data, say of customers as anything other than an asset.

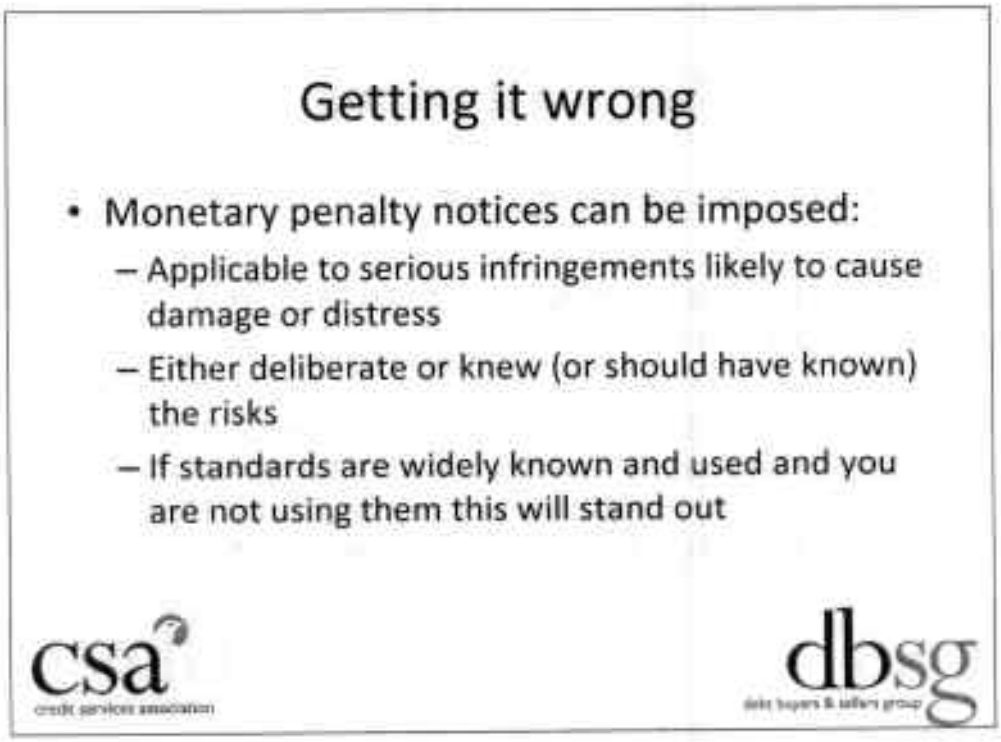
If someone is trying to steal it via hacking or if its loss is newsworthy or detrimental to individuals, it clearly has a value.

Whether you have assigned a monetary value to your data, or a value in relation your reputation, it's time to take a look at risk.

The loss of any data that you maintain, particularly if that data contains information subject to regulatory control carries a certain amount of risk if that data were to be lost, damaged or stolen. As you accumulate more of that data, the risk of loss goes up.

So analyse the risk versus return: If you're not getting a return on your data but it presents you with significant risk, should you hold on to it?

The ultimate financial risk may paying a monetary penalty to the ICO...



MPs are a last resort but have been used – majority of cases relate to security breaches

Was it serious?

How much data did you lose?

How sensitive was it – how likely to cause damage or distress to the people that the data referred to? Could be loss of money, could be distress caused by harassment, for example by mistracing

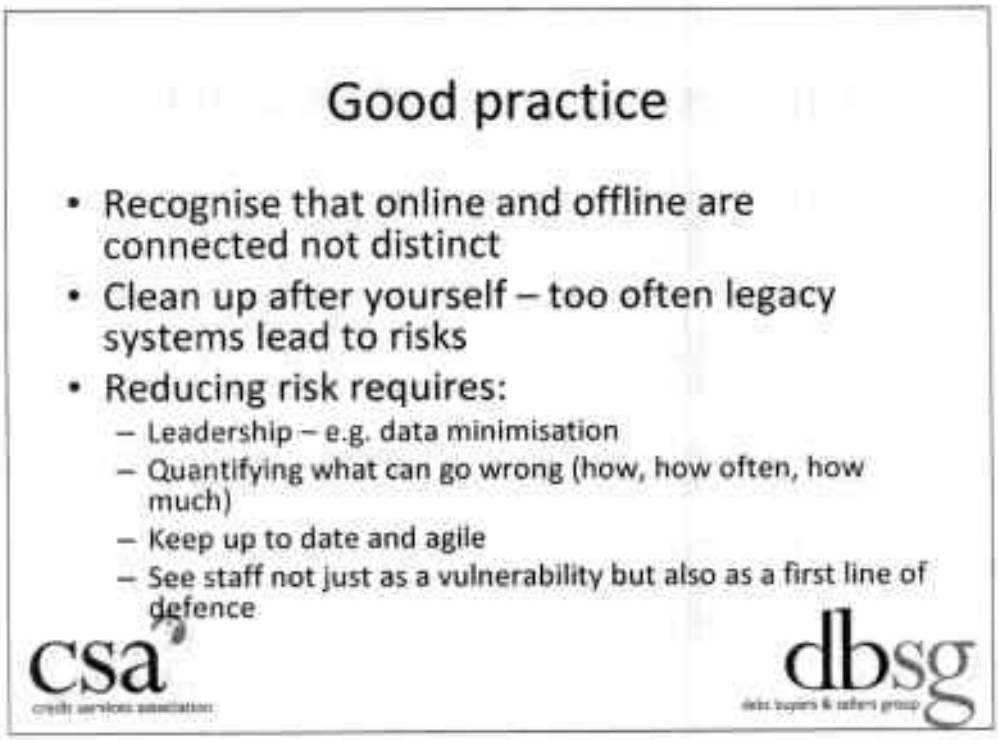
Risk assessment vital – if you don't know what can go wrong and how bad it could be, how can you show the ICO that a breach was not caused by negligence?

The ICO does not require that a data controller adopts a particular standard, rather that they put in place security measures that guard against the level of risk that exists bearing in mind the nature of the personal data they process and the nature of the processing.

Recent case is Lush – they weren't fined because they did take some reasonable steps but they should have done more – next time a monetary pen is much more likely

Does your business take this seriously?

Quote is from Sally Poole re Lush case – same goes for anyone though, not just retailers and not just online (which leads to next slide....)



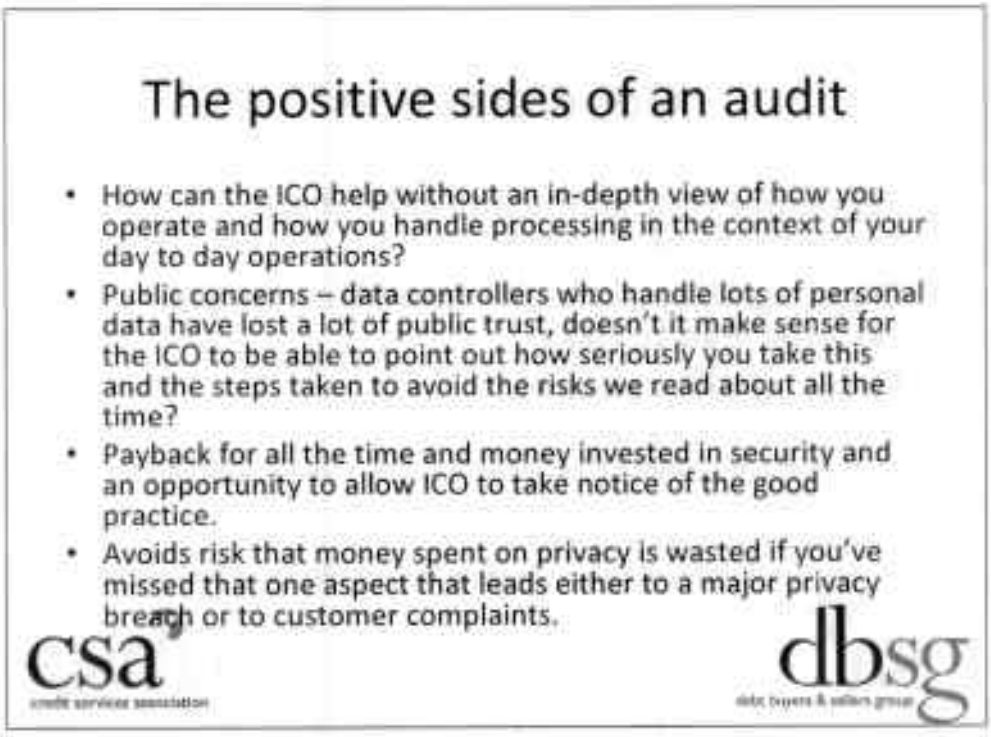
Think of security as a whole not just as discrete bits of the business – think of the data journey/lifecycle, where it comes in, how it's used, who sees it, where does it go? Don't sit back and think the website is secure because your physical premises might not be. Egs useful (staff training etc)

Adding more processing without getting rid of things you don't need anymore increases risk

Leadership – who is willing to tell the business that this data isn't good enough or we don't need it?

Just because something worked last year doesn't mean it's any good now

Listen to staff concerns ("I can never find what I need" might also mean "We don't know where we keep things and can't therefore know whether it's safe"



The audit function is there to help

Not identify potential enforcement cases

Compulsory audits in public sector/Not in private

A way of rebuilding trust for data controllers with previous breaches?

Be sure that the investment in security has paid off or identify where more is needed.

An audit covers the full spectrum of security, identifies potential chinks in the armour when assessed as a whole

Not simply a technology audit – governance (policy and procedures, physical security assessed, records management, staff training, also assessed

- Subscribe to our e-newsletter
- at www.ico.gov.uk

- Follow us on Twitter
- at www.twitter.com/iconews

csa
credit services association

dbsg
debt buyers & sellers group

Upholding Information Rights: A Data Protection update from the ICO

David Smith
Deputy Information Commissioner

6th Sept 2011

Where are we now?

- Information Rights Strategy consultation
- More integrated
- Improved efficiency and effectiveness
- Using new powers and penalties
- Where it's at
- Looking to the future

ico.

Information Rights Strategy

- Integrated approach
- Our goal, purpose and outcomes
- Enforcing; promoting good practice; educating and informing; influencing
- Maximising our impact
- Our tactics
- Importance of independence

ico.

Protection of Freedoms Bill

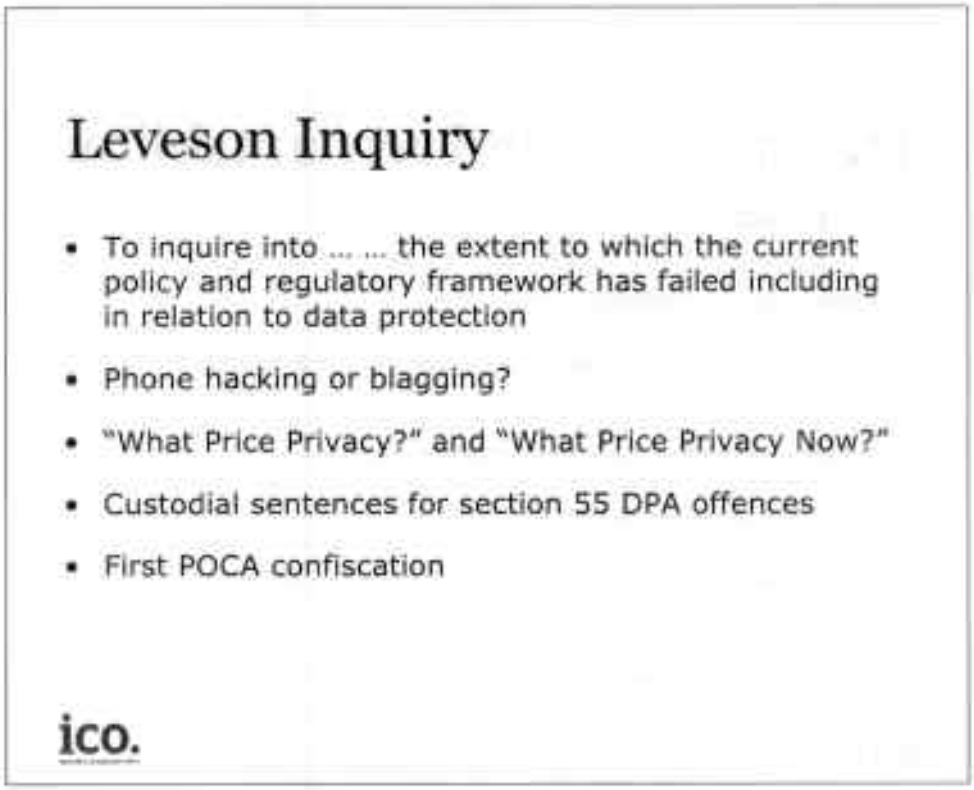
- ICO independence
- Regulation of biometric data
- Regulation of surveillance
- Safeguarding vulnerable groups, criminal records etc.
- Vehicles left on land

ico.

Transparency and accountability agenda

- Open data consultation
- Commitment to preserve privacy and protect personal data
- Anonymisation and pseudonymisation
- Crime mapping example
- Forthcoming O'Hara report on privacy and transparency
- Possible ICO Code of Practice

ico.



General Approach

strengthening our teeth – no longer a "toothless tiger" but education, awareness, encouraging good practice still our primary focus;

retaining our commitment to "strengthening public confidence in data protection by ..... simplifying and making it easier for the majority of organisations who seek to handle personal information well, and tougher for the minority who do not" (if you want to keep this);

committed to principles of good regulation:

regulatory activities should be carried out in a way which is transparent, accountable, proportionate and consistent;

regulatory activities should be targeted only at cases in which action is needed;

developing risk based processes – based on minimising risk to individuals and society through improper use of personal information;

working with other regulators to ensure joined up approach, no double jeopardy etc;

international co-operation on cross border enforcement eg case we referred to Spanish DPA on marketing of timeshare led to fine of 60,000 euros.

Powers and penalties

- Civil monetary penalties
- Five penalty notices issued
- Increased audit activity
- Summary reports published
- Positive feedback and lessons learned

ico.

Changes to the Privacy and Electronic Communications Regulations

- Additional supervisory powers
  - Monetary penalties
  - Audit
  - Information notices
- Mandatory breach notification
- New rules for cookies
- ICO advice published

ico.

Future legal framework

- Reviews of international instruments
- European Commission proposals awaited
- Regulation or Directive?
- Harmonisation or light touch regulation?
- What other changes can we expect?
- What is worrying you?

ico.

Keep in touch

Subscribe to our e-newsletter at www.ico.gov.uk
or find us on...

www.twitter.com/iconews

ico.

Information Commissioners Office – Update 2011
Ward Hadaway

David Clancy
Investigations Manager
Information Commissioner's Office

Sept 2011

Content.

- Privacy Electronic Communications Regulations 2011
- The ICO powers and how it will affect your organisation
- How the Regulations affects cookies
- Data Protection and privacy, the future
- Monetary Penalties and review of recent cases

ico.

Overview

- Recent changes to the Privacy and Electronic Communications (EC Directive) Regulations 2003

- Cookies and similar devices

- The Commissioner's approach

ico.

Privacy and Electronic Communications Regulations

Intended to 'particularise and complement' DPA

Provide specific rules for:

- Processing of traffic and location data
- Cookies and similar devices
- Direct marketing by electronic means (phone, fax, email)

Can apply to corporate subscribers and in situations where no personal data is being processed

Where personal data DPA rules will also apply

ico.

Changes to the Regulations - 2011

- European Directive on which the Regulations are based amended (implications for all EU countries)

- UK government implemented changes through the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

Key changes in the UK from 26 May 2011:

- New rules for those using cookies or similar devices
- Changes to the Information Commissioner's powers to enforce the Regulations
- Specific requirements for 'service providers' to notify the ICO of personal data security breaches

ico.

Commissioner's new powers

- Power to serve a **monetary penalty of up to £500,000** on organisations that seriously breach the rules:

  Where the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the organisation must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

- **Third party information notices**

ico.

Use of cookies and similar devices

- Rules apply to storage of information or access to information stored in the terminal equipment of a subscriber or user
- Since 2003 – had to provide clear and comprehensive information about cookies and provide 'opt out' opportunity
- New requirement – to provide clear and comprehensive information and obtain consent from subscribers or users
- No consent required where cookie is strictly necessary for the provision of service requested by the subscriber or user

ico.

Mixed reaction

"EU unleashes the cookie monster"

"Is this the Way the Cookie Crumbles?"

"Will the cookie crumble?"

"Does your website take the biscuit?"

"Beware of this new, half-baked cookie law"

ico.

ICO approach

- Recognise the challenges of implementing these requirements
- 12 month period from 26 May 2011 for organisations to comply
- Flexibility in guidance for organisations to find best way of meeting these requirements in their circumstances
- At this stage we expect organisations to be able to set out a realistic plan to achieve compliance
- Some areas where clear there will be particular challenges – third party cookies

ico.

Going forward

- Will continue to work with industry and European colleagues to address difficult areas
- Keen to hear from you about practical suggestions and solutions
- Will develop and add to our cookies guidance as we become aware of innovative solutions or suggestions
- Update of 'Personal Information Online Code of Practice'

ico.

Data protection & privacy, the way forward

Consent

- Art 29 Working Party Opinion 15/2011 on the Definition of Consent
- "unambiguous consent"
- Data controllers must be able to demonstrate consent
- Quality and accessibility of information on which consent is based
- Suggestions re minors and those with limited legal capacity

ico.

Data protection & privacy, the way forward

Issues

- Control – data subject should be in control of the use of their data
- Transparency
- Freely given – no deception, intimidation, coercion or significant negative consequence if he/she does not consent
- Specific – must relate clearly to the scope and consequences of the processing in question
- Informed – must be based on an appreciation of the facts an implications of an action

ico.

Data protection & privacy, the way forward

Issues – continued

- Timing – sensible to obtain consent prior to the start of processing
- Withdrawal of consent – decision taken on the basis of prior consent cannot be annulled, however, if there is no other legal basis for storing data is should be removed
- Legal capacity – there is an acceptance that the rules do not provide legal certainty. The WP believe the review of the Directive should address this. An example could be a sliding scale approach whereby the type and use of data would determine the level of consent (representatives input)

ico.

Review of the Data Protection Directive

New Challenges

- Technological developments
- Globalisation
- The collection of data is now more complex and less detectable

ico.

Key objectives

- Strengthening individuals rights
- Increasing transparency
- Enhancing control over one's data
- Ensuring free and informed consent
- Protection sensitive data (should genetic data be included)

ico.

Key Objectives

- Making remedies and sanctions more effective
- Reducing the administrative burden
- Clarifying the rules on applicable law
- Encouraging self regulation and exploring EU certification schemes
- Clarifying rules for international data transfers
- Promoting universal principles

ico.

Enforcement Action
Monetary Penalties

Cases

- Hertfordshire CC – fax breach (100k)
- A4e – loss of unencrypted laptop (24,000 datasets) (60k)
- Surrey CC – misdirected emails on 3 occasions (120k)
- ACS Law – online attack led to security breach on website (1k)
- Ealing & Hounslow Councils – unencrypted laptop (80 &70k)

ico.

Prosecutions

Cases

- T- Mobile Hames & Turley – ordered to pay confiscation cost of £28,700 and £45.000 failure to pay within 6 months would result in 18 months and 15 months prison sentence

- Campbell – NHS employee passing patient information to accident claims company employee - £1,050 fine

ico.

Contact details

David.clancy@ico.gsi.gov.uk

01625 545877

ico.

Keep in touch

Subscribe to our e-newsletter at www.ico.gov.uk
or find us on...

facebook

twitter

www.twitter.com/iconews

YouTube

LinkedIn

ico.