Dear Ollie Simpson

BCS Response to the Ministry of Justice
The Knowing or Reckless Misuse of Personal Data – Introducing Custodial Sentences

Thank you for inviting BCS, the Chartered Institute for IT, to respond to the above consultation. BCS has repeatedly expressed concern over the damage to citizens of misuse of their personal data and we agree that the government should introduce custodial sentences for offences knowingly and recklessly committed under section 55. This should send a signal to those intending to commit such offences and profit significantly from them, and to the general public who need to feel that this threat is taken seriously.

BCS promotes wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 70,000 members including practitioners, businesses, academics and students, in the UK and internationally. We deliver a range of professional development tools for practitioners and employees.

A leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.

We hope that you will find our comments (which follow and in the attached questionnaire) of assistance and would be delighted to discuss these further, if you wish.

Yours sincerely

Ian Ryder
Deputy Chief Executive,
BCS, The Chartered Institute for IT
Tel: +44 (0)1793 417750
Appendix: Further explanatory notes and background to accompany the questionnaire (attached as a separate document)

*** PLEASE NOTE ***

This document is a discussion of the issues, and should not be taken as legal advice or a commentary on any specific incidents in the past or future.

Summary

To understand the issues raised by a custodial sentence for recklessness, a number of points must be explored:

- The protection of personal information is a matter of significant public interest and concern. In the context of single large scale incidents of data breaches, the current interpretation of the law has little impact on IT practitioners who have control of the systems containing personal information.
- The introduction of custodial sentences for offences under section 55 of the DPA could provide a route to prosecute IT practitioners who have acted recklessly, resulting in a single disclosure that is harmful.
- It is unclear what constitutes either disclosure or misuse in this context.
- Key to this issue is how ‘reckless’ is defined in the context of professional behaviour. There is precedent in other professions, and a clear understanding that with professional status there is responsibility that may not be avoided by claiming ignorance. There is, however, no clear definition of what would constitute recklessness for an IT practitioner.
- The impact of the threat of prosecution and incarceration could be positive or negative. If IT practitioners can operate without qualifications, and adding qualifications brings criminal liabilities, there is a clear incentive to remain unqualified. However, if professional status provides routes to demonstrate proper behaviour and properly avoid prosecution, the incentive could be very positive; the impact on behaviour could be highly beneficial to the public.
- There is a duty of care to ensure that professionals acting reasonably do not end up convicted or even prosecuted because of ill-defined requirements and expectations.
- The prosecuting authority and professional body have important roles to play in ensuring that frameworks exist around the law to support good professional behaviour. A gradation of sanctions could lead to avoidance of the most serious negligence and recklessness, and widespread adoption of good practice.

Further explanation of the above points continues below, along with recommended areas for further investigation.
Catastrophic data loss and the law

Personal information disclosure and misuse is a matter of significant and growing public concern, and there is both individual harm and wider societal damage inflicted when it occurs.

Since 2006, there have been a number of significant – some might say catastrophic – data losses that have received public attention through the media. Most of these cases have been isolated incidents as far as the organisations involved were concerned. It may be suggested that the enforcement notices under section 40 resulting from these breaches were superfluous; the data controllers in question would have been under considerable pressure to take all necessary measures to prevent further losses with or without an enforcement notice. For the subjects of that personal information, the damage is already done and unaffected by the enforcement notice.

Regardless of impact after a breach has occurred, the provisions for enforcement notices provide no direct incentive for the prevention of isolated incidents, only the prevention of chronic repetition. In terms of criminal offences, an organisation must repeatedly ignore notices and unofficial communication from the ICO for a prosecution to be brought. Since 2006, Liverpool City Council and ADC Organisation Ltd are the only two prosecutions under section 47 (failure to comply with a notice) – according to ICO annual reports. This compares with around 30 prosecutions under section 17 (failure to notify of processing) and eight under section 55 over the same period.

In practice, current prosecutions target repeat infringers of DPA principles, and those who knowingly and intentionally disclose or misusing personal information for their own benefit. Professionals who are reckless in the management of personal information leading to significant public harm do so without fear of prosecution.

Section 55 of the DPA and reckless professionals

A path may be taken through section 55 of the DPA as follows:

‘A person must not recklessly, without the consent of the data controller, disclose personal data…’

A data controller may properly procure or otherwise commission an IT system to be developed, implemented or maintained to store personal information, and reasonably expect the system as used to be appropriate to the task. If the individuals engaged to provide or maintain the system act in a manner that is reckless, it is reasonable to assume they do so without the consent of the data controller. In that case, if personal information is disclosed as a consequence of recklessness by those implementing or maintaining an IT system, it is possible that a prosecution could be brought against them under section 55 – perhaps leading to a custodial sentence.

What is ‘disclosure or misuse’ in this context?

One element that requires a clear legal definition is what constitutes a ‘disclosure’ or ‘misuse’. A natural assumption would be that publication online with no protection would constitute disclosure. Personal information could also be published online with a protection – such as a document password that is a dictionary word – that would be easily and simply revealed with readily-available
tools. Would that constitute disclosure? This is clearly open to a wide interpretation, with wildly different implications for practice depending on what is established through precedent.

**Professional recklessness**

For a prosecution of the kind in question to be considered under section 55 of the DPA, behaviour must be ‘reckless’. In context, the individual may well be regarded as reckless if they behave in a way that knowingly involved unnecessary or inappropriate risks.

There are precedents in other professions. Members of recognised professions acting in the domain of their expertise do have a different set of expectations placed on their actions. A professional is expected to be competent to a basic level in their domain, and to recognise and act within their own limitations – lack of knowledge within that domain is no excuse for those identified as professionals. Conversely, if a professional can demonstrate that they are competent and used good practice, this may be an adequate defence against adverse consequences.

This is clearly established in the medical profession: If a medical professional is unaware of a published contra-indication for a treatment, then harm resulting from their treatment of a patient against that indication may be their responsibility regardless of whether they were aware of the issue. If a medical professional appropriately prescribes a licensed pharmaceutical in accordance with guidelines then they may have acted properly whether or not the patient is harmed by an adverse reaction. However, a healthcare practitioner who provides treatment beyond their level of capability and/or authorisation may be responsible irrespective of whether the treatment would be regarded as appropriate when prescribed by someone who was authorised.

Similarly, an IT Professional who uses good practice in securing a system containing personal information should not be held responsible for breaches that were either unforeseen or regarded as acceptably low risk. However, anyone specifically engaged to provide IT systems or services to store personal information who fails to take basic precautions could be in difficulty.

Yet without a test through the courts, it is impossible to predict what level of practice would secure against a charge of ‘recklessness’. It may, however, be useful to speculate on what the IT Profession itself may regard as reckless. For example, it is vitally important for online systems to be kept up to date with operating system and application patches. There are good systems in place for updating operators on vulnerabilities and distributing fixes or advice notes. A failure to adhere to this minimum standard of practice when maintaining a system containing personal information could conceivably be considered as reckless.

There is a continuum of behaviour, from putting personal information online without any real protection (for example at an unpublished URL) and hoping for the best, through to leading edge privacy and security technology and practice. Somewhere on that continuum there is a line below which behaviour will be regarded by the courts as reckless. That line may vary depending on the circumstances, but it is highly likely that a proportion of current practice in the UK will fall clearly below that standard, putting the individuals involved at risk of prosecution.
**Deterrence or perverse incentive?**

The threat of prosecution for failing to meet a bare minimum of practice could encourage IT practitioners to raise standards. That is not, however, guaranteed. It could also create an incentive to either avoid responsibility, or avoid qualifications and professional status that could remove ignorance as a defence in court.

It is reasonable to expect that the capability, qualifications and status of individuals involved in managing personal information could be taken into account when deciding if a particular behaviour is (or would be) reckless. Greater capability means a higher expectation. In mature and established professions the answer is simple – that those who are not qualified and demonstrably capable are prevented from taking critical actions and decisions. In the IT sector, provable qualifications and professional status is not yet sufficiently widely adopted or part of the culture. BCS is working to promote proper qualification and professional status, focusing around the Chartered IT Professional status (CITP), and in many areas this is becoming part of the culture.

The crux of the issue is whether individuals in key positions of professional responsibility for personal information are expected (or required) to have expertise in proportion to their role. If so, it is reasonable to regard basic failures as potentially reckless irrespective of formal qualifications. If, however, it is legitimate for someone engaged in a particular IT role to claim ignorance of basic measures then that is highly problematic.

In ideal circumstances it would be reasonable to suggest that a data controller commissioning services should ensure that those engaged are appropriately qualified, but there is no incentive for them to do so currently. The situation may evolve where data controllers are absolved from responsibility by delegating to an IT practitioner without any qualifications; any breach would formally be without their consent. The IT practitioner is absolved by a lack of qualifications. The effect would be that the public could have no expectation that their personal information was being adequately protected.

**Duty of care towards the professional**

There is of course no desire from BCS to see a flurry of prosecutions of IT professionals carrying out their normal duties. It is vital that those who wish to act with due diligence and care are given the tools to do so. Clarity is required on what would constitute negligence, gross negligence and recklessness in circumstances where the ultimate sanction is imprisonment – and that clarity is required *before* any prosecutions take place.

Risks may be reduced, but not eliminated. It is possible for personal information to be protected with the best possible known practice, but an unknown or extremely unlikely risk may still bring about a breach. A professional who has acted properly should not feel threatened by the prospect of a prosecution even if the information in their charge is disclosed or misused. They should be in a position to know what good practice is, and how to document the decisions made to demonstrate that good practice was used. They should have confidence that this will be recognised by the courts, by prosecutors, and by investigators; they should be confident they will not find themselves in court, let alone convicted.
The role of the prosecuting authority and the professional body

The prosecuting authority – in this case the ICO – has a role to play in setting guidance. This can take the form of high level explanatory guidance on legislation, and can involve outlining good practice. The ICO have a great deal of guidance available, and tools like Privacy Impact Assessments have their place.

There are a number of requirements for a profession to be publicly recognised, one being a code of conduct that is publicly available and actionable. Members of BCS sign up to such a Code of Conduct (that can be found at http://www.bcs.org/server.php?show=nav.6030) and action can be brought against those who contravene it. The Code includes sections on public interest, duty to relevant authority and competence that addresses the issues around personal information both through general principles that apply and as a specific case.

This creates the potential for a hierarchy and response escalation that ensures good practice becomes the norm, and protects practitioners from straying into recklessness.

This hierarchy could evolve along these lines:

<table>
<thead>
<tr>
<th>Behaviour</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘reckless’</td>
<td>Knowing failure to implement basic practice that results in a disclosure of personal information leading to significant actual or likely harm</td>
<td>ICO prosecution leading to custodial sentence</td>
</tr>
<tr>
<td>‘gross negligence’</td>
<td>Failure to implement basic practice irrespective of a disclosure or harm</td>
<td>Misconduct complaint leading to removal of professional status</td>
</tr>
<tr>
<td>‘negligence’</td>
<td>Failure to implement known best practice</td>
<td>Misconduct complaint leading to formal censure, suspension or reduction of professional status or other measure as appropriate</td>
</tr>
</tbody>
</table>

Over time this would create layers of appropriate precedent and definitions such that both practitioners and the courts would have a great deal to inform any decisions on what constituted professional recklessness. There would be the added benefit that the materials and precedents produced by the professional body – i.e. BCS – would support the prosecuting authority – i.e. the ICO – and ensure that they would not be required to go into overburdening detail on good practice. Furthermore, the structures of a professional body include publications that constantly debate and update good practice and ethical behaviour in this context amongst the professionals themselves.

In a steady-state the baseline of practice would be such that action for negligence is relatively rare, and prosecution for recklessness no more than an annual occurrence. A side effect would be that IT professionals are able to stand their ground more effectively when instructed to act inappropriately – as established professions are also able to do.
Fair and appropriate liabilities

The argument outlined above deals with the issue of professional recklessness *without the consent of the data controller* in isolation. Adjacent to this issue there are other offences that may require similar penalties – such as reckless or negligent behaviour by the data controller. There are complex relationships between individual and corporate liabilities, and the role of directors/trustees. It is important that there are interlocking liabilities that fairly reflect the roles and responsibilities.

For example, an IT practitioner may send a memo outlining their concerns over safety of a system or process to the relevant data controller. If that is acknowledged or overruled, then that IT practitioner may be free to act because they do so with the consent of the data controller. The practical implications for a data controller for accepting such a memo are unclear.

It would also be unreasonable for an IT practitioner to face the possibility of a criminal prosecution for recklessness when their own authority is limited and/or judgement overruled by general managers.

Areas for further examination

The key questions for further examination are:

- What other offences carrying similar sentences are necessary to create full interlocking liabilities for individuals and organisations, such that responsibilities and accountabilities are fair and harmonised?
- Are there obvious legal guidelines that may be established for what constitutes recklessness, disclosure and misuse in this context?
- What opportunity, incentive or duty is there in practice for the prosecuting authority to undertake prosecutions of this kind?
- What is required in order to ensure that the threat of prosecution is beneficial? – for example, guidance from the Ministry of Justice, ICO and Director of Public Prosecutions
- What is required from the professional body in order to support the above?
- What steps need to be taken when to ensure a good outcome?
- How should this be communicated?

Ian Ryder
Deputy Chief Executive
BCS, the Chartered Institute for IT

December 2009