Response to Consultation Paper CP22/09
"The knowing or reckless misuse of personal data - Introducing custodial sentences"

Q1. Should the Secretary of State introduce custodial penalties for offences committed under section 55 of the DPA?

Do custodial penalties actually deter?
The assumption that custodial sentences deter first offenders, based on the concept of the offender as a rational actor who weighs rewards and consequences in accord with classical economic theory, is being quite widely challenged, even among advocates of custodial sentences. For example, Saunders and Billante state "*prison does not work wholly, or even mainly, by its deterrence effect. It works most crucially by physically removing the worst offenders from society so they cannot go on committing crimes (that is, by incapacitation)*" (Saunders and Billante, A view from sociology, Policy 19, 2, 2003, p. 64).

There is little conclusive evidence either way on whether custodial sentences deter re-offending, except that some studies suggest dependencies on the nature of the offence, the age group and social background of the offender. No substantive work seems to have been conducted on the impact of custodial sentences in relation to the specific kind of offence under discussion here, but there are plenty of documented instances on record where custodial sentences have not deterred re-offending on the part of "white collar" offenders in general.

So in the absence of evidence that custodial sentences are effective as a deterrent, they should be reserved to those cases where they serve usefully to incapacitate offending.

What are the primary causes and effects of personal data leaks?
The reality is that the majority of significant-scale leaks of personal data so far recorded in the UK have been primarily caused by inadequate data management policies on the part of the Data Controller rather than individual negligence or intent on the part of a person acting "without the consent of the data controller," - indeed in the now-infamous HMRC incident the Data Controller was subsequently demonstrated to have overridden the very proper concerns of the individual who performed the ultimate act that resulted in the data loss.

Very little actual societal harm has so far been traced directly to even the most egregious bulk data leaks. While numerous individual cases of fraud can readily be traced to card skimming and phishing, even the massive loss of credit card data by TJX in 2007 did not precipitate a detectable boom in card fraud, nor did the various UK government leaks of the same year result in identifiable secondary crime waves. Even the recent telecoms customer data leak - despite potentially being a section (55)(4) offence, i.e. intentional unlawful obtaining and supplying of personal data for gain, has apparently resulted in little more than the possibility of customers getting some unwanted sales calls from other providers.

So while there is legitimate public concern (which the author strongly shares) about leakage of personal data, any response must be appropriate to the real nature and proportionate to the real scale of the problem.

How effective has the 1998 Act been so far?
Excluding the period between April 2006 and March 2007 for which the author could find no figures, since April 2000 there have been 78 prosecutions under the 1998 Act and the transitional arrangements under the 1984 Act. Of these 32 have been for section 55 offences, all of which have resulted in convictions. That equates to a mean of about four prosecutions per year. Given the lack of policing (the ICO essentially relies on complaints) and the weak link between data leaks and identifiable repercussions on data subjects, it

would be most surprising if the identified section 55 offences were more than the pinnacle of an iceberg primarily consisting of minor breaches. Indeed a survey just published by Cyber Ark suggests that over 40 per cent of office workers in the financial sector have taken sensitive data when they moved to a new job (http://www.net-security.org/secworld.php?id=8534).

Sentences have included absolute discharge (1), conditional discharge (4) and fines ranging from £50 to £200 per count, the maximum aggregate fine being £3200 for 44 counts of obtaining and 44 counts of disclosing (2007).

The current low rate of detection and prosecution, and the trivial penalties so far applied provide an insufficient body of evidence upon which to base decision-making on such an important matter as the introduction of custodial sentences. Although serious penalties might reasonably attach to systematic and large-scale misuses of personal data, given the uncertainties discussed above it is highly questionable whether further increasing the population of our already overcrowded prisons is a justifiable response to individual minor breaches of section 55.

Is the existing law granular enough?
DPA section 55 subsumes several rather disparate offences, so the lack of granularity in the relevant provisions of both DPA and section 77 of the Criminal Justice and Immigration Act 2008 (CJIA) raises cause for concern.

In the case of negligent or reckless disclosures (which so far dominate the leak landscape) the nature and degree of the negligence or recklessness should be a paramount consideration in sentencing. For example, an employee losing an unencrypted laptop containing personal data where the employer provides and requires the use of the laptop but has made no provision for encryption cannot justly be considered as culpable as in the case where the employer has provided the encryption but the employee has not made use of it, or where the employee has taken it upon him- or herself to use a personal device without the employer's instructions or knowledge.

A particular concern is accidental disclosure from systems in the temporary care of persons such as consultants and contractors acting under the general instructions of a Data Controller. For example, breaches of Internet facing systems under live test might fall within the definition of "reckless" and result in such an individual receiving a custodial sentence regardless of the limited control they might have been permitted to exercise to mitigate or minimise the chance of a breach. Therefore, in the case of reckless disclosure, a graded tariff based on the full circumstances of the case is the only approach that would seem provide a reasonable chance of just outcome.

Where wilful disclosure without a financial motive is demonstrated, the matter is obviously simpler, but rather than applying a standard custodial sentence in all cases, it would be more just and more cost-effective to again apply a principle of proportionality to sentencing that reflects the resulting harm.

Solely in the case of seeking to profit financially from disclosures in contravention of section 55, a fixed tariff would seem appropriate. A custodial sentence is however unlikely to be the most appropriate option, given the lack of evidence of its efficacy as a deterrent against either offending or re-offending in this category of crime and the disproportionate cost to the public purse of short-term incarceration.

So, weighing the full social cost of custodial sentences carefully against the prospect of actual harm caused by the offence and the lack of evidence relating to deterrence, it is moot whether a custodial sentence, and particularly a relatively short custodial sentence, is an optimum choice in this context.

In any case it seems improper to migrate directly from the patently ineffectual deterrent offered by the current trivial penalties to a potentially disproportionate penalty such as two years imprisonment without serious investigation of whether some less extreme increment might prove sufficient.

The author therefore believes it is premature to introduce the custodial sentencing provision of CJIA section 77, which seems to have been drafted without adequate consideration of its potential efficacy or its side effects, very much as a "knee jerk reaction" to the embarrassment resulting from some recent high profile breaches.

Q4. Defence for anyone who can show that he was acting for the special purposes with a view to publishing journalistic, literary or artistic material ...

The author is strongly in favour of a public interest defence, subject to proportionality of the scale and nature of the disclosure to the level of public interest. However the restriction of purpose to "publishing journalistic material" is unnecessarily narrow, and could tend to inhibit legitimate "whistleblowing" where there is no intent to "publish" in the journalistic sense.

Given the narrowness of the "journalism" restriction, the author finds the inclusion of a "literary or artistic" purpose in this defence quite bizarre. The implied assumption that such disclosures and purposes can fulfil a "public interest" purpose sufficiently to serve as a legitimate defence has no merit. "Being of interest to the public" does not equate to public interest.

The equivalent exemptions under section 32 of DPA refer to legitimate data processing by Data Controllers, and as such have merit in relation to literary and artistic purposes, as absent the exemptions it would be effectively impossible, for example, to conduct research for an unauthorised biography of a living person. However, in the context of a section 55 offence, relating as it does to an action on the part of a person who is by definition in breach of their statutory duty to the Data Controller, such an exemption cannot be justified.

Summary

The author's general view is that both provisions of CJIA section 77 are too crudely formulated and inflexible make good law. As presented they ignore the maxim that "circumstances alter cases" - which is probably more valid in this context than many, given the diverse ways in which personal data leaks can occur in our highly technologised society.

The current detection rate for offences under DPA is too low for any sound conclusions to be drawn regarding patterns of offending or re-offending, and the current penalties are so negligible that a deterrent effect is patently improbable, even should such an effect be theoretically possible. Therefore enforcement may be better served in the first instance by more effective policing than by imposing extreme penalties. Only once the detection rate has improved enough to provide a statistically significant body of evidence should the level of penalty be reviewed on the basis of that evidence.

The exemptions need to be completely revised, encompassing as they do in a single "all or nothing" clause both the appropriate but unduly restrictive and the utterly unjustifiable.

Above all, we must keep in mind that the aim of the legislation should be to reduce offending whilst satisfying the basic principle of proportionality that underlies justice in a democracy. Neither vengeance nor political muscle flexing have any rightful place in the legal process.

Michael Barwise
Director

mbarwise@intinfosec.com