Privacy and criminal records

Comparing the British and Australian experience

By Sylvia Song

***Silvia Song** (B Econ, LLB (Hons)), is currently studying a Master of Laws in Computer and Communications Law at Queen Mary University of London, and works as a Legal Director at an incorporated legal practice.*

In the days following the Google Spain case[1] thousands of 'take down requests' were made, more than half of which were from Europeans with criminal convictions[2]. This reflects the inherent conflict between an individual's right to privacy and the public interest in crime in the community.

In this paper, this conflict is discussed in the context of comparing data protection laws between Australia and the UK. The United Kingdom as a member of the European Union is required to harmonise its laws with those of Europe. The arguable danger with moving towards a 'continental' position, is that privacy lacks a doctrinal basis in English common law[3], and further may increasingly reflect laws which are out of step with public opinion.

Although Australia shares a similar common law heritage with English law, it is less exposed to the influence of European laws. Although both the UK and Australia have laws protecting criminal records, this is changing in England, where cases in light of European data protection and human rights laws have pulled the country towards a more continental view of privacy.

Contrasting the treatment of criminal records

The view one takes on the public interest of disclosing and retaining criminal records varies largely from country to country. Sex offender names and addresses are publicly available in the United States, whereas in the UK (and Australia), criminal records are generally only accessible by law enforcement authorities and courts, and are subject to spent conviction or step-down laws.

In European civil law countries by contrast, criminal histories are generally considered private and confidential. In Spain for example, the concept of 'personal honour' and privacy are more fundamental rights than the public interest in knowing an individual's criminal history. Thus Spanish courts have ruled it in breach of the Personal Data Protection Law to post on the internet the names of police and civil guard officers guilty of torture (or awaiting such prosecution)[4], or the name of a police officer convicted for sexual assault[5].

Courts in Europe do not necessarily public or allow access to judgments. This is in contrast to common law systems such as Australia, where "*the conduct of proceedings in public is an essential quality of an Australian court of justice*"[6]. Some common law systems such as the US stress the public benefit in increasing safety in the community, as a right paramount over an individual's privacy.

> *"Most Americans would find the Spanish (and European) 'right to honor' quite strange, especially to the extent that it prevents disclosure of information about convictions… Why should the state guarantee that a convicted person can keep his image clean and integrity unblemished?... [w]ide dissemination of conviction information arguably enhances public safety because it allows people to avoid convicted criminals or take precautions in their business and social interactions with them".*[7]

The UK regime

Criminal records are included in the definition of 'sensitive information' in the UK Data Protection Act 1998 ("**the Act**")[8], requiring a higher level of protection. It is an offence for employers to require employees to make a subject access request for criminal records in order to share it with the employer (section 56).

Under the EU Data Protection Directive[9] (on which the Act is based), criminal records are not 'sensitive information' that would require explicit consent for processing. Article 7 of the Directive therefore requires unambiguous consent or other legitimate bases for processing of such information. Relevantly, Article 8(5) authorises complete registers of criminal convictions to be kept only under the control of official authorities.

The right to privacy arises from Article 8 of the European Convention on Human Rights ("**ECHR**" or "**Convention**") as an individual's "right to respect for his private and family life". This may not be interfered with except for in the public interest or as required by law. The Convention was implemented into UK domestic law with passage of the Human Rights Act 1998.

Criminal records certificates cases

The ECtHR recently found the disclosure of an old police caution to be in breach of Article 8 of the European Convention on Human Rights ("**the Convention**") in the *Case of MM v United Kingdom*[10]. Here the subject's criminal records certificate (now DBS certificate) disclosed a caution for the child abduction of her grandson for one night[11]. The Court recognised the need for a comprehensive record of information, however Article 8 was engaged given the absence of safeguards for their review and deletion. What was important was the ruling in relation to retention of such information:

> *"199. [T]he indiscriminate and open-ended collection of criminal record data is unlikely to comply with the requirements of Article 8 in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, inter alia, the circumstances in which data can be collected, the duration of their storage, the use to which they can be put and the circumstances in which they may be destroyed."*

Although the Convention has been implemented into domestic law with the passage of the Human Rights Act 1998, the ECtHR's judgment is at odds with earlier judicial authority in the UK.

The Court of Appeal in October 2009 decided that retaining a complete register of convictions was consistent with national law and the Directive. In *Chief Constable of Humberside Police*[12], an appeal by five chiefs of police was upheld against a notice to delete certain criminal records from the police national computer (PNC). Considering spent conviction laws[13] prohibiting disclosure of old offences, the court decided that there should not be any analysis of whether activities fell within police "core purposes", as the police were the best judge of their needs.

Given that courts and other public bodies (such as child protection authorities) were entitled to the information, the full information should be held (even regardless of police purposes). LJ Waller commented that if the policy were to be applied consistently, the judgment would require the deletion of around a million convictions. Hence such laws should not be overruled by operation of the Directive:

> *"[I]n certain circumstances this information will be disclosed, but that is because Parliament has made exceptions to the Rehabilitation of Offenders Act. What is more, the circumstances in which there will be disclosure are circumstances in which the Data Subject would be bound to give the correct answer if he or she were asked. <u>It is not as it seems to me the purpose of the 1998 Act to overrule the will of Parliament by a side wind</u>."* [at 44, emphasis added]

Similarly and regarding the proposed 'step-down' regime or some other type of limited access, Lord Justice Hughes made the point that such a regime "*is not to be achieved through the Data Protection Act*" (at 113).

The leading authority on criminal records disclosure remains Lord Woolf CJ in *R v Chief Constable of the North Wales Police ex parte Thorpe*[14]. The Chief Justice provided the rationale why disclosure was justified against a couple who had committed sexual offences against children:

> *"Both under the Convention and as a matter of English administrative law, the police are entitled to use information when they reasonably conclude this is what is required (after taking into account the interests of the applicants), in order to protect the public and in particular children… where the use in question is decided upon as a result of the exercise of an honest judgment of professional police officers, that will of itself, go a long way to establish its reasonableness." (at 429)*

Lord Woolf generally endorsed accepting police judgment in relation to disclosure, meaning that the weight of English authority favours the needs of law enforcement in any particular case.

The Australian experience

Australia's system of privacy and data protection rules derive from the federal *Privacy Act 1988* (Cth). However, all states and territories have also separately enacted privacy laws (with the exception of South Australia and Western Australia)[15].

Personal information is defined in section 6 as:

> "*…information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable."*

Some commentators have found the scope of the definition as not having been examined in depth "*due to the unsatisfactory lack of information privacy related jurisprudence*"[16]. This definition may be wider than that of 'personal data' in the EU Data Protection Directive given that it also covers opinions about an individual's information, whether true or not.

The federal legislation requires entities to have a privacy policy, and abide by the Australian Privacy Principles (APP's). These principles deal with information use and disclosure, transparency, the collection of solicited and unsolicited personal information, and notification requirements. The principles also deal with data quality, security, onwards transfers of information, and access to information.

Relevantly, the exception relating to law enforcement is APP 6.2(e), which allows an organisation to use information for any other purpose than the primary reason it was collected, unless the entity reasonably believes that its use or disclosure "*is reasonably*

necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body."

Criminal records information in Australia

With regards to criminal records information, the Australian legal system is similar to the UK. Individuals have a right of non-disclosure of spent convictions[17] for less serious offences if the sentence was for less than 30 months imprisonment and more than ten years ago. There are some limitations to its application[18], and notably the legislation excludes employers reviewing a person's suitability to work with children. Courts and law enforcement agencies also have the right to this information, as does security and other agencies[19].

Although convictions are public, unless there is information in the public domain about old convictions (such as on the internet, like in Google Spain), it would be difficult and time-consuming to find it. Criminal background checks are generally only carried out by the individual (as is also the case in the UK).

There are relatively few cases on the topic of criminal records information, or indeed testing the limits of the Privacy Act. The few decided cases however highlight the possible direction should it become more common for individuals to request the deletion of their information as is currently gaining momentum in the UK.

In the case of *Coffey v Centrelink*[20], the Federal Court considered whether the Privacy Act was infringed by the retention of a record of criminal charges concerning the applicant by the South Australian state police ('SAPOL'). There was no state privacy legislation in force at the time, and the subject charges had long since been withdrawn.

The policy of the South Australian Police (SAPOL) was to place minor offences into an inactive file after five years. This policy was criticised with their practice given that the charges were withdrawn and were in any event of a minor nature and were in excess of ten years old (at 10-11).

Justice Mansfield expressed some dissatisfaction at the retention of the so called "records" and found it inappropriate to present the information as a criminal record.

> *"In the circumstances, I can well appreciate his frustration at the information still held by SAPOL concerning those charges. It is hard to see any justification for the retention of such records. Apart from their availability to government agencies being unregulated by law, they are available to the public subject to the controls of the Freedom of Information Act 1991 (SA). It is in any event entirely inappropriate that the information maintained should be presented on a document entitled 'Offender History'. Mr Coffey is not an 'offender' against any provision of any statute in respect of the charges." (at 38)*

The court expressed disapproval at the practice of retaining information of charges that did not lead to any convictions, and dismissed the application on other grounds. This was upheld upon appeal[21]. At the time of judgment in 2004, the court noted that four of the seven states/territories of Australia (being Queensland, New South Wales, Western Australia, Northern Territory, and Commonwealth) had spent convictions legislation allowing for expungement of certain criminal records.

It would be preferable if the issue were decided in a straightforward manner according to such spent convictions legislation, and that there would be no perceived conflicts with the Privacy Act, as alleged by the European Court of Human Rights in the case of *MM v United Kingdom*. This would give effect to the legislative intention of these laws, rather than a circumvention via a "side wind" as alluded to by LJ Waller in Humberside.

The attitude of the Australian Privacy Commissioner is evident in a case concerning a disclosure by a marine park to the news media of an individual's unlawful breach of park rules. In *'EQ' and Great Barrier Reef Marine Park Authority*[22], an individual had broken marine park rules by fishing unlawfully, and the leaked story resulted in the publication of personal information in connection with the alleged offence. The individual alleged interference with privacy that caused him non-economic loss.

The Commissioner found a prima facie breach of the privacy principles, as the marine park had not yet issued the penalty. However damages were awarded in the amount of $5000, given the complainant's own fault in the matter.

The exemption for disclosure to enforcement bodies was considered in the case of ''EZ' and 'EY'[23] This was a complaint to the Privacy Commissioner of a Doctor's disclosure to a police officer to the effect that their patient "might be psychotic, but would require further assessment". The privacy principle (NPP 2.1(h), as it then was) allowed an organisation to disclose personal information where use or disclosure was "reasonably necessary" for the prevention or investigation of criminal activity.

The Commissioner found a prima facie interference with privacy which did not allow reliance on the exception, given detailed health sector guidelines on this issue. This finding can be contrasted against the earlier case of *Jones v Office of the Australian Information Commissioner*[24], where the Federal Court upheld lawful exercise of the exception by a psychiatrist served with a police warrant to seize records.

Conclusion

The Australian experience with criminal records and privacy laws has been measured. On the issue of retention, the judgment in Coffey illustrates that the court will review the circumstances surrounding retention as well as the information itself. The medical records cases also illustrate that any disclosure believed

to be for the prevention of crime will be scrutinised in light of patient confidentiality.

In contrast, the experience in the United Kingdom is of a creeping approach towards the European or "continental" view of criminal record retention as a breach of privacy. The United Kingdom was found to be in breach of data protection laws by the European Court of Human Rights where retention as well as disclosure were ruled an interference with Article 8 rights.

This judgment stands in direct conflict with previous Court of Appeal authority and requires a consideration also of the landscape around rehabilitation and conviction laws. This is starkly evident in the change of policy requiring retention of cautions, following the Soham murders and resultant inquiry.

English courts have warned against the overriding of such validly enacted rehabilitation laws by using data protection laws as a "side wind". It can only be hoped that the British experience will prove educational for Australian regulators and judges in determining the precise privacy that should be afforded to criminal records. The fundamentality of court transparency and openness, as well as the lack of civil law notions such as "right to honour" should weigh against following the European judgment of MM.

---

[1] *Google Spain SL and another v Agencia Española de Protección de Datos* (AEPD) and another, [2014] 3 W.L.R. 659f, where the European Court of Justice (CJEU) affirmed an order by the Spanish data protection agency that Google remove links relating to an individual's past financial debts.

[2] Hakim, D. 30 May 2014. *The Right to be Forgotten? Not that Easy.* The New York Times. Page B1.

[3] as generally accepted in English case law, see Phillipson, G. (2003) *Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act*. Modern Law Review 66(5): 726-758.

[4] Tribunal Supremo (Sala de lo Contencioso-Administrativo, Seccion 6a, 26 June 2008), as quoted in Jacobs, J. and Larrauri, E. 2012. *Are criminal convictions a public matter? The USA and Spain.* Punishment & Society 14(1): 3 – 28, at 21.

[5] Sentencia de la Audiencia Nacional (10 February 2010), as quoted in Jacobs & Larrauri, (see no. 5 above)

[6] Judicial Commission of NSW, http://www.judcom.nsw.gov.au/publications/benchbks/civil/public_proceedings.html

[7] Above, no. 4 at page 18-19.

[8] Section 56, Data Protection Act 1998 (UK)

[9] Data Protection Directive - *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*

[10] *Case of MM v The United Kingdom* 24029/07 HEJUD [2012] ECHR 1906

[11] In 2006, a policy change applied to require all adult cautions to be retained for life, in relation to offences where the injured party was a child. This followed the 2002 murder of two schoolgirls in Soham, England, and Birchard Report of 2004.

[12] *Chief Constable of Humberside Police & Ors v The Information Commissioner & Anor* [2009] EWCA Civ 1079

[13] Section 4, *The Rehabilitation of Offenders Act* 1974 (UK)

[14] [1999] QB 396

[15] *Privacy and Personal Information Protection Act* (1998) New South Wales; *Information Act* 2002 (Northern Territory); *Information Privacy* Act 2009 (Queensland); *Personal Information Protection Act* 2004 (Tasmania); and *Privacy Data and Protection Act* 2014 (Victoria); *Information Privacy Act* 2014 (Australian Capital Territory). South Australia has an administrative instruction in place. Note that the Western Australian Information Privacy Bill 2007 has not yet been passed by state Parliament.

[16] Burden, M. and Telford, P. 2010. *The Conceptual Basis of Personal Information in Australian Privacy Law*. eLaw Journal: Murdoch University Electronic Journal of Law. 17(1), at 27.

[17] Part VIIC, Division 6 of the *Crimes Act* 1914 (Cth).

[18] Note that state offences must still be disclosed if to any person other than a Commonwealth authority.

[19] See also Regulations 7A and 8 and Schedule 3 of the *Crimes Regulations* 1990 (Cth).

[20] [2004] FCA 188 (5 March 2004)

[21] *Coffey v Centrelink* [2004] FCA 233 (16 August 2004)

[22] [2015] AICmr 11 (2 February 2015)

[23] [2015] AICmr 23 (27 March 2015).

[24] [2014] FCA 285