The right to privacy, the right of national security and the challenges posed by new technology in the UK and China

The purpose of this paper is to examine how the right to privacy is protected under UK and Chinese law and how new technology is increasingly encroaching on the protection and enjoyment of this right. The paper will be divided into four short sections. In the first section, I will look at UK legislation on the right to privacy and examine some of the recent high-profile court cases in which new technology has been found to have impeded that right. In the second section, I will assess how Chinese law seeks to protect individual privacy from the ever increasing reach of new technology. In the third section, I will examine the extent to which the expansion of new technology represents a perceived threat to national security and how both Chinese and UK law allows the state to override the right to privacy, often through the use of new technology. In the final section, I will suggest some ways in which Chinese law might benefit from UK privacy laws within the wider context of new technology.

This will include a review of a recent landmark court case, which found in favour of a claimant whose privacy was breached over the internet. In the third section, I will examine the extent to which the expansion of new technology represents a perceived threat to national security and how both Chinese and UK law allows the state to override the right to privacy, often through the use of new technology. In the final section, I will suggest some ways in which Chinese law might benefit from UK privacy laws within the wider context of new technology.

But before doing any of this, it is important to remind ourselves exactly what we mean by the right to privacy. As we already know, the right to privacy is a universally recognised human right which occupies a central position in the international human rights doctrine. For example, Article 12 of the 1948 Universal Declaration of Human Rights states that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation'. Article 17 of the 1966 International Covenant on Civil and Political Rights says almost exactly the same thing. And, of course, Britain and China have signed both of these documents.

But when these documents were first drafted, the ability of technology to impinge upon individual privacy was probably limited to some very basic forms of phone bugging that would involve someone breaking into your house and installing a rather clumsy and poorly concealed network of wires that were connected to your old-fashioned landline telephone. Not so anymore. Similarly, the idea that people had rights to “on-line” privacy such as the right to communicate privately by electronic mail or the right not to have one’s personal details made publicly available on the internet was simply non-existent back then. How things have changed.
Right to privacy in the UK - law and practice

If we start then with UK law, the right to privacy is protected by a variety of different legislation. One of the most important for the purposes of this paper is the Data Protection Act. This was enacted in 1998 to bring UK law into line with a 1995 European Directive requiring Member States to safeguard the right to privacy with regard to the possession of personal data, usually held on computer databases. Among other things, the Act imposes limits on what companies can do with data relating to their employees or customers, and what public bodies can do with data relating to people in their care or under their control. It also gives members of the public the right to access information being held about them. My students have the right to see what I write about their essays and dissertations through the Data Protection Act. Breach of the Act can be both a criminal and a civil offence. The usual sanction is a heavy fine, although imprisonment can also be levied.

The Law of Confidence gives the individual a right to privacy in “tort”. This a civil action taken by one citizen against another under common law, a type of law developed by judges through decisions of court rather than through legislation. In seeking to prove that this right has been breached, a claimant must show that the information made public about him, often using new technology, was strictly confidential and that the person or organisation that disclosed the information had a “duty of care” not to do so. The successful claimant will be entitled to financial damages at the discretion of the judge.

The 2000 Regulation of Investigatory Powers Act governs the interception of postal and electronic communications, including emails and telephone calls, and makes it a criminal offence and a civil wrong – “in the absence of lawful authority” - (which are key words) to intercept such communication without the consent of both the sender and the recipient. Sanctions for breach of this act include a fine and/or imprisonment of up to two years.

Examples of how new technology has been used to breach the right to privacy in the UK are innumerable and some of the cases that have come to court are very high-profile indeed. Only very recently we have had the phone-hacking scandal, involving the News of the World, a British tabloid newspaper published by News International which is a subsidiary of News Corporation owned by Rupert Murdoch. Several employees of the newspaper are accused of using technology to listen in to private conversations in order to publish articles based on these conversations. Initial police investigations back in 2005/6 concluded that the paper’s phone-hacking activities were limited to targeting celebrities, politicians and members of the royal family. However, in July this year, it was revealed that phones belonging to the relatives of deceased British soldiers and victims of the July 2005 London bombings were also accessed by News of the World journalists. The resultant public outcry led to a mass boycott by advertisers and the closure of the paper after 168 years of publication.

Police investigations are still taking place. A number of arrests have been made and a number of high-profile resignations have been tendered, including Sir Paul Stephenson as Commissioner of the Metropolitan Police, following speculation about his involvement with one of the arrested News of the World journalists. Custodial sentences seem likely. Following the earlier phone-hacking scandal of 2005/6, Clive Goodman, then Royal Editor of the News of the World and his associate, the private detective Glenn Mulcaire, were imprisoned for four and six months respectively after pleading guilty to unlawful interception of communications brought under the Regulation of Investigatory Powers Act noted earlier, so UK law clearly takes breaches of privacy via technology very seriously indeed.

In terms of breaches of the Data Protection Act, in 2010 a fine of £60,000 (RMB 630,000) was imposed on the employment agency A4e Limited when a laptop containing unencrypted personal data relating to over 24,000 people who had registered with the company was stolen from the house of an employee. Also last year, a fine of £100,000 (RMB1,000,000) was imposed on Hertfordshire County Council (in the south of England) for twice sending child abuse documents intended for counsel to the wrong fax number. Neither case involved anyone...
acting malevolently. These were acts of carelessness. But the severity of the fines illustrates the importance attached to the protection of “on-line” privacy in the UK.

The tort of confidence is much harder to prove (as with most tort law cases) but Max Moseley, former president of the Formula One governing body the FIA, was successful. Here again, the case involved The News of the World. The paper published photographs of Moseley engaged in sadomasochistic practices with a Nazi theme, after one of the paper’s employees posing as a guest, secretly used video technology to film Moseley on his private property. Moseley took the paper to the High Court in 2008 on a number of counts, including breach of privacy, and was awarded £60,000 (RMB 630,000) in damages.

**Right to privacy in China – law and practice**

Privacy laws in China will be familiar to most of our Chinese audience, so I don’t intend to spend too much time outlining what most of you will probably know already. But just briefly, unlike the UK, China, of course, has its own constitution and although the most recent 1982 Constitution does not expressly grant a right to privacy, it does set out several provisions which seek to protect privacy. For example, Article 37 protects individual freedom from unlawful search of their person, Articles 38 and 39 provide that personal dignity and the homes of citizens are inviolable and Article 40 safeguards privacy of correspondence.

The 1986 General Principles of Civil Law recognises a general right of reputation (Article 101), but does not provide for privacy as an independent right. Although the Supreme People’s Court sought to clarify this point in Article 140 of its 1988 “Opinion”, it merges the right to privacy with the right to reputation such that the victim of a breach of privacy – whether this is breached on-line or otherwise - cannot sue to protect his privacy unless his reputation has also been harmed.

In terms of rights to “on-line” privacy, Article 7 of the 1997 Computer Information Network and Internet Security, Protection and Management Regulations (“Computer Information Regulations”) states that ‘the freedom and privacy of network users is protected by law’ and that ‘no unit or individual’ can use the internet ‘to violate the freedom and privacy of network users’. Similarly, Article 36 of the 2010 Tort Liability Law imposes joint and several liability on any network user and network service provider that violates the privacy of another person via the internet.

Recent case law in China suggests that the courts are beginning to recognise a right to the protection of privacy from violation by new technology, although there is nothing like the abundance of cases that we have seen in the UK over the years. The first such case in China came in 2008 which I will call the Wang Fei case (Wang Fei v Zhang Leyi, Daqi.com and Tianya.cn, Beijing Chaoyang District Court, No. 10930). The claimant, Wang Fei, took legal action for invasion of privacy against Zhang Leyi and two local website operating companies, Daqi.com and Tianya.cn. The facts of the case are as follows.

Wang Fei’s wife, Jiang Yan had committed suicide after discovering that her husband was having an extra-marital affair. Shortly afterwards, Jiang’s university friend Zhang Leyi created a website in remembrance of Jiang and as a place for relatives and friends to post their condolences. The website contained personal information about Wang Fei, including his name, address, employer and some photographs of him. Zhang Leyi also posted some articles describing the chronological events that led to her friend’s death. Visitors to the website copied the material to other websites and discussion boards, including those hosted by the defendants Daqi.com and Tianya.cn. Daqi.com made a social analysis of the incident and invited public comments and discussion. The consequence of this was a lot of bad feeling against Wang Fei, who received on-line and face-to-face death threats and was forced to resign from his advertising job. The Chaoyang District Court found in favour of Wang Fei, although Wang only received RMB8,000 rather than the RMB135,000 that he was claiming. Despite this rather paltry return, the case
itself is significant because it was the first to decide in favour of a claimant for “on-line” breach of his right to privacy.

The right to privacy and national security
Moving now to the tension between the right to privacy and issues of national security, both Chinese and UK law empowers the state to supersede or “trump” the right to privacy if there is a perceived conflict between the exercise of that right and the perceived interests of the nation. Dealing with China first, if we look at state constitutions, each of the four promulgated since 1949 has contained a single, all-encompassing provision which forbids the individual from exercising his rights in a way that infringes upon ‘the interests of the state, of society and of the collective’ (Article 51 of the 1982 Constitution). If we apply this article to the debate at hand, it allows the Chinese state to use technology to impinge upon the right to “on-line” privacy, by for example using specialised equipment to view private email correspondence or to listen in to telephone conversations. The article can also be invoked to override conventional rights to privacy through the use of technology - for example, by seizing personal data that is stored on computer.

Looking at rights to “on-line” privacy as specifically referred to in Chinese legislation, we noted earlier that Article 7 of the Computer Information Regulations prohibits ‘units and individuals’ from violating the privacy of network users. But the article is noticeably silent on whether or not the state can do so. Article 4 of the Regulations provides guidance as to why. This article prohibits any individual from using the internet ‘to harm national security, disclose state secrets and harm the interests of the State…’. Presumably, therefore, anyone who is deemed to have done so, irrespective of whether or not his is exercising his right to “on-line” privacy as enshrined in the Regulations, will find that this right is overruled by the state. Article 15 of the Internet Information Services Regulations 2000 imposes a similar obligation on network service providers, forbidding them from disseminating information that ‘endangers national security’ or ‘goes against the basic principles set in the constitution’. It is very clear from this that state’s interests take precedence over the on-line privacy of the individual.

And there are similar laws in the UK. We noted earlier how the Regulation of Investigatory Powers Act prohibits the interception of correspondence, including emails and telephone calls, without the consent of both the sender and the recipient. But the Regulations don’t prevent the state, or more accurately the police, from doing so provided they have ‘lawful authority’. How do the police obtain lawful authority to intercept correspondence? By procuring an “interception warrant” from the Secretary of State allowing them to seize communications if it is ‘in the interests of national security’ or ‘for the purpose of safeguarding the well-being of the United Kingdom’ (Section 5(3) of the Regulations). The UK’s 2008 Counter-Terrorism Act goes one step further in that it giving the police powers of surveillance if they suspect someone of being involved in terrorist activities. This invariably involves using technology to carry out the surveillance of private meetings or to view private email correspondence.

All of this leads us to the inevitable question of how we interpret what is meant by “national security” or the “national interest” and the circumstances under which we might be able to justify using technology to overrule rights of privacy in this context. Article 51 of the 1982 Constitution is particularly susceptible to criticism. This type of all-encompassing article places unrestrained authority in the hands of the Chinese government since it is the government that determines what is meant by the national interest and the government that revokes any constitutional rights, including privacy rights, that are adjudged to conflict with the national interest. With this in mind, it does not seem unduly harsh to suggest that what the Chinese Government defines as the national interest is quite simply what is the best interests of the Chinese Government.

But UK law is also vague on defining the national interest and also on defining who is considered to be a threat to the national interest. Exactly who falls into the category of terrorist, for example, is not altogether clear. Islamic fundamentalist, dissident Irish republicans and right-wing extremists would be the most obvious examples, but what is to stop the state from broadening its definition of terrorist much wider than this and using technology to spy...
on anyone that it loosely suspects of being a terrorist? Although not directly linked to the rights of privacy, the police did use technology surveillance techniques in wrongly identifying the Brazilian plumber Jean Charles de Menezes as a terrorist the day after the July 2005 London bombings. On the basis of this surveillance, the police then followed him to a London tube station and shot him seven times in the head.

What is to be done?

On a slightly lighter note, the written guidance for this conference asks European participants to propose solutions to a lack of legal capacity in China based on the European experience. I’m not sure if I have any ready-made “solutions” as such, but there are a couple of areas of UK law that might at least interest our Chinese delegates.

The first is probably well known to all of you already – a data protection act. The consensus among Chinese legal theorists that I know and whose works I have read is that China desperately needs a data protection law to protect individuals from public disclosure of personal information. It may well be possible to take out a case under the 2010 Tort Liability Law, but proving a case in tort is never easy and it would be much more straightforward and logical to promulgate an act dealing specifically with the protection of personal data. We have seen how UK law comes down very hard on negligent companies or public bodies that violate data protection laws and China needs something similar if it is serious about modernising its legal system.

Another area of UK privacy law that is interesting if not altogether essential or even desirable for China, is what we call “super-injunctions”. As far as I know, the only types of injunction that exist in China are restraining orders preventing people from repeat-offending or “preliminary injunctions” preventing further infringement of intellectual property. The super-injunction is something different and is increasingly used in the UK to prevent tabloid newspapers from publishing stories about individuals who don’t want these stories made public. This is usually because the stories are embarrassing. The England footballer John Terry was initially successful in obtaining an interim super-injunction preventing the News of the World from publishing a story about his affair with a team mate’s ex-wife. His attempts to renew the injunction failed, however, and needless to say he is no longer on speaking terms with this former team-mate! Like, John Terry, the former Wales footballer Ryan Giggs was also successful in securing an interim super-injunction preventing the News of the World (again!) from publishing a story about his extra-marital affair with a former beauty queen. But this was leaked, ironically, using new technology – twitter! It was then published in a Scottish newspaper on the grounds that the injunction only covered the laws of England.

Clearly, we can’t take super-injunctions too seriously. They are very much the domain of the rich because they are incredibly expensive to obtain. That said, I can only imagine that with the increased intrusiveness of independent commercial media in China, there are a number of Chinese celebrities who have secrets that they’d rather keep to themselves!

Robert Weatherley
Associate
for Mills & Reeve LLP
+44(0)1223 222338
robert.weatherley@mills-reeve.com

www.mills-reeve.com T +44(0)844 561 0011

Mills & Reeve LLP is a limited liability partnership regulated by the Solicitors Regulation Authority and registered in England and Wales with registered number OC326165. Its registered office is at Fountain House, 130 Fenchurch Street, London, EC3M 5DJ, which is the London office of Mills & Reeve LLP. A list of members may be inspected at any of the LLP’s offices. The term “partner” is used to refer to a member of Mills & Reeve LLP.

The contents of this document are copyright © Mills & Reeve LLP. All rights reserved. This document contains general advice and comments only and therefore specific legal advice should be taken before reliance is placed upon it in any particular circumstances. Where hyperlinks are provided to third party websites, Mills & Reeve LLP is not responsible for the content of such sites.