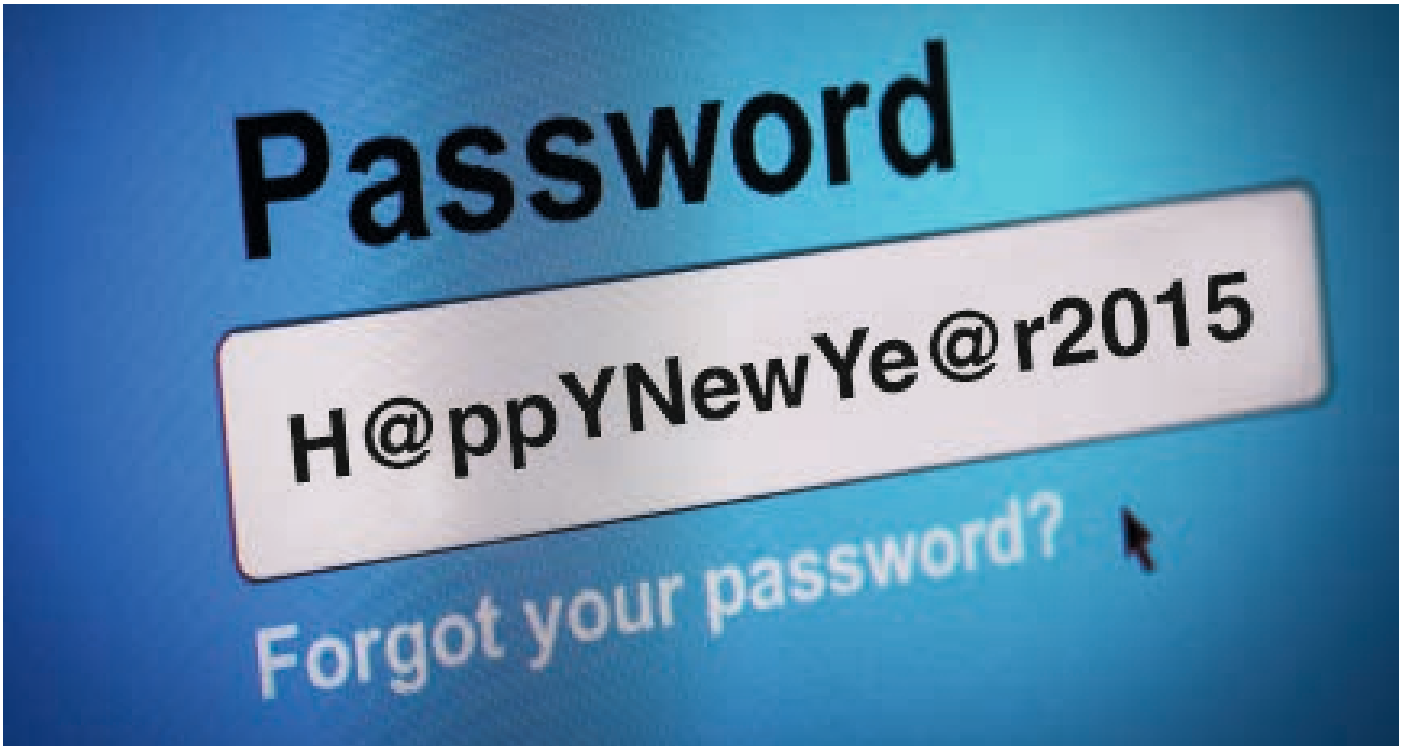

Private eye

Tom Morrison returns with his quarterly review of the world of information law

IN BRIEF

- A big year for anniversaries.
- The Triennial Review and legislative changes are on the horizon.
- Idea for an easy New Year's resolution: change your password.

2015 is a year for anniversaries. A ridiculous comment perhaps as by their nature all years are a year for anniversaries. What I mean is that as we start a new year having just celebrated the 30th anniversary of England and Wales' first—albeit largely irrelevant—Data Protection Act, we are now commemorating 10 years of the full force of the Freedom of Information Act 2000 (FIA 2000). I have not got my dates wrong; it took five years to implement. This ground-breaking piece of legislation was far from irrelevant—how can anything described by a former Prime Minister as one of his biggest mistakes be irrelevant—and it marked a new era for the right of the public to know more about the decisions public authorities make in all our names.

March also represents the fifteenth anniversary of our first genuinely meaningful piece of data protection legislation—the Data Protection Act 1998 (DPA 1998—which took nearly two years to be activated). DPA 1998 was a watershed for the protection of personal freedoms. It put in place a matrix of rights which would flex as the world evolved from a silicon age to the information age. Perhaps equally as importantly April marks the fifth anniversary of the introduction of civil monetary penalty notices, or put in more common sense terms, the right of the Information Commissioner to impose fines of up to £500,000 without having to first take a wrongdoer to the courts.

A quick search around the Internet confirms that 2015 also marks 750 years since Simon de Montfort's parliament and 800 years since the sealing of Magna Carta. More than pertinent to the subject matter of this column, but I will leave that for more capable authors to cover.

So what else is coming up this year?

The Information Commissioner's Office (ICO) will hold its annual Data Protection Practitioner Conference in Manchester. None of us needs a crystal ball to know that the conference will be oversubscribed, because it provides what has proven in the past to be one of the year's best opportunities for practitioners to hear what the ICO and other speakers have to say about the evolving world of information law and practice. A must-attend event, if you can get a ticket.

Video footage will be somewhere near the centre of privacy concerns. We now have a Surveillance Camera Commissioner (SCC) who published his first annual report at the end of last year. He has confirmed his intention to promote the Surveillance Camera Code of Practice to authorities covered by the Protection of Freedoms Act 2012 as well as trying to convince non-relevant authorities to adopt of the code voluntarily. Retail centres and education providers are described as the Commissioner's "single biggest challenge".

Sticking with cameras, new guidance has been issued on the use of drones. It is likely that Father Christmas has delivered a job lot of the little flying things over the Christmas period and that those which are not currently stuck in trees as a result of unfortunate piloting will be getting ready for their next surveillance operation. Avoiding the potentially frightening consequences of a drone being ingested by a jet engine (please be careful anyone who lives near an airport), drones present an opportunity for some fun. They also present an opportunity for snooping and can carry more sinister connotations. The ICO has reminded the public of its CCTV guidance; whilst wholly personal use is unlikely to be subject to DPA 1998 it is good manners if nothing else to pay heed to the common sense guidelines.

Review of legislation & the ICO

The Ministry of Justice (MoJ) will complete its triennial review of the ICO. The public has been invited to respond to a questionnaire by 16 January 2015 with the stated aim of identifying the ICO's key functions and considering how best they can be delivered, including whether they should continue to exist at arm's length from government. Assuming the review concludes that the ICO should continue in its current form, the MoJ will consider improvements in efficiency and governance terms. Triennial reviews are not a tick box exercise; they are meant to ensure that non-departmental public bodies are necessary and effective, but it would be surprising if the MoJ concludes that the Information Commissioner should not be independent, or at least kept arm's length, from government especially in light of previous criticism from the EU.

The Draft Data Protection Regulation will probably not be passed. This has been a slow but fierce burn. After the economy, information rights is one of the hottest topics for the EU. The accompanying debate has not led to speedy reform. Perhaps part of the problem is that the law—as enacted and enforced in the UK at least—is not as broken as some may lead us to believe. Of course it can be improved, but it works and is protecting citizens in the modern age despite having been written when some offices were still using typewriters. A new, directly applicable Regulation is likely to hit us at some point, but not as soon as some had hoped or expected.

The law on nuisance calls and spam texts will probably be strengthened. The Department for Culture, Media and Sport has conducted a consultation on proposed changes to the Privacy and Electronic Communications (EC Directive) Regulations 2003. The desire is to make it easier for the ICO to fine companies making nuisance calls, or sending spam texts in light of a case which saw its popular decision overturned in a case involving several hundred thousand spam texts on the basis that the legal threshold required to issue a fine had not been met. There is widespread support for change among government and consumer groups, so it seems inconceivable that the change will not be made.

Enforced subject access will be banned. This should have happened years ago but for various reasons the law has sat frozen on the statute books for a decade and a half. A typical example of enforced subject access is where a business "asks" a job candidate for to submit a subject access request to the Police. The prospective employer is not really asking, it is saying "if you want this job you have to submit the request and show us the results". Employers do not ask the question for no good reason though; indeed for some roles there is a compelling public safety argument for it. Equally there is an obvious public interest in the rehabilitation of offenders. The problem is that subject access is intended to protect individuals, not the public. We have a separate regime for employers, now operated by the Disclosure and Barring Service (DBS), to run a controlled mechanism with built in safeguards. Employers can ask individuals to go to the DBS via Disclosure Scotland without breaching the enforced subject access provisions (when they come into force) but the results will be limited to unspent convictions and cautions. For roles where a more detailed background search is appropriate, there is an existing regime of enhanced DBS checks available to relevant employers. The law was due to have changed on 1 December 2014, but got held up with a last minute glitch. We are told that it will come soon.

New Year's Resolutions

I ended the previous edition of this column looking at how emerging technologies carry privacy implications, but that there is a balance to be struck for each of us in terms of convenience versus protection. The two are evidently not mutually exclusive. The intersection between convenience and protection is the area where businesses can differentiate themselves and add real value to their products and services. While we as individuals are often critical of organisations who jump the lights at the intersection, it is individuals who are often the worst offenders.

There is no doubt that someone's password will be hacked this year; thousands have probably already been compromised by the time you read this. There were some high profile instances of user accounts being breached and systems being accessed last year as a result of users' poor password habits. The consequences are sometimes severe, but they are nearly always inconvenient.

Nobody likes having to type long passwords with a m1xTure% of upper case and punctuation, but fewer like having to be on the phone with the bank explaining why we think our accounts have been accessed without permission or trying to reconstruct our online identities once taken over by a stranger. Information subsists online but it also lives on the portable devices we use every day. If you have not got a passcode on your phone, tablet and laptop, then I would agree that it would be a better use of your time to stop reading right now to add one.

If you want an idea for an easy-win feel-good New Year's resolution then change your default password now and make it a bit more complex. If you are feeling brave then come up with variations on it and use different passwords for different applications, on the basis that if one password is compromised then the fallout is confined to that one service. If you are feeling virtuous then go for 2FA, but if you know what that means you have probably already got it! **NLJ**

Tom Morrison, partner, Rollits LLP (*tom.morrison@rollits.com; www.rollits.com*)