Notes from CILIP Privacy Briefing

Held CILIP 28th November 2017

The day attracted delegates from a wide range of sectors including academic, public, and notably archives and specialist collections. Provided a focus on Privacy in the context of evolving technology and regulations such as GDPR.

Chair's Introduction

CILIP trustee Martyn Wade chaired the day and introduced the programme with a reminder that privacy is a human right enshrined in the European Convention on Human Rights (ECHR Article 8) and the UN Universal Declaration of Human Rights (Article 12)

Although CILIP is currently reviewing its code of ethics, the current code stresses confidentiality and privacy as a core principle and value of the profession (principle 8).

Yet the current direction of travel and adoption of technologies tends to lead society away from these principles of personal privacy. What is the role of LIS professionals in this arena?

- Educators (informing our patrons of the issues particularly around technologies)
- Purchasers (expecting fair and transparent behaviour from our suppliers)
- Providers (modelling privacy conscious behaviour in our own practice)
- Advocates (speaking out for better regulation and practice)

Privacy, surveillance and the information profession: challenges, qualifications and dilemmas? David McMenemy – University of Strathclyde

Privacy defined as:

> *The right to be free from unwarranted intrusion and the keep certain matters from public view*

Although this right is recognised under the ECHR (see above) there are some exceptions in cases when governments can interfere:

- In accordance with the law and is necessary in a democratic society
- In the interests of national security
- For public safety or the economic wellbeing of the country
- For the prevention of disorder or crime
- For the protection of health or morals
- For the protection of the rights or freedoms of others

But none of these are clear-cut statements. It is about balancing the individuals right to privacy against these other concerns. The issues and arguments are nuanced

But for LIS professionals this is our professional space and we shouldn't ignore it.

We need to DEBATE and DISCUSS these issues both in general in our profession but also in specific instances and situations within our own practice. We may decide on occasions that other concerns outweigh the privacy concerns but there needs to have been a thought process rather than an unthinking acceptance. Technology should not drive professional values – we always need to be able to justify our practice and decisions.

Nissenbaum presents one perspective on these issues proposing a "Framework of Professional Integrity" which can be used to explore potential situations where privacy may be invaded through our LIS services and practice.

This involves thinking about the following in a situation:

- Context
- Informational norms (how does information flow, be communicated)
- Actors (Senders and recipients of information and the subject of the information)
- Attributes (what kind of information is it -who need access to it)
- Transmission principles (What are the rules about who can access, when, why)

Each of these areas need to be considered in evaluating any specific instance

LIS professionals need to be able to stand behind and defend professional ethos not just see it as a set of desirables. This will challenge our practice if we tackle issues in an honest manner.

Are you ready for GDPR? Benjamin White – British Library

Benjamin introduced the session by describing the current situation in the UK around privacy and data law as being draconian with the situation made worse by a lazy press who only react to legislation which affects our privacy if a high-profile example of the results of these laws becomes visible.

There was a reminder that data protection law relates to personal data which has to be:

- Something that allows you to identify a living individual
- An opinion about an identifiable living person (they need not be explicitly named if it is obvious from your description who they are!)

Sensitive personal data especially protected.

The driving principle is that the data should be protected where it has the potential to cause damage or distress.

You need to have particular reasons (legal basis) for making use of personal data and infringement can be punished by considerable fines – as well as reputational damage.

Changes in GDPR and what we need to do:

- Registration no longer required as accepted that all organisations hold personal data.
- Ensure your privacy notices are transparent using plain English (Granny Test) and clearly explain what data is going to be used for and what will happen to it.
- Document your processes involving personal data (Who, What, Why, Where, How)
- Privacy Impact Assessment – How do you store data, who can access, what are chances of a breach, how could we improve our systems?
- "Legitimate Interests" ground is being removed from regulations in GDPR – everything has to be in the interests of the subject rather than the data holder.

If you are an Archive service then different rules apply because it is in the nature of an archive that material being held may well go against the interests of living individuals. If everyone could "opt-out" or have their material destroyed the integrity of the archive would be destroyed.

Protecting Citizen's Privacy in your Library - Aude Charillon - Newcastle City Council

Aude shared her experiences of raising the issues of privacy in practical ways at Newcastle Public Library.

Crypto Party: Held at Newcastle Public Library looking at various apps and tools which can be used to protect your privacy online.

About 15 attended each event but tended to be people already in the know and wanting to look at tools in more detail or have a debate about them.

Needed to reach a broader audience

How do we teach privacy by stealth?

Include in the digital skills training sessions.

Useful tools include:

Library Freedom Project http://frama.link/ToonsLibsPrivacy Training

8 Day Data Detox http://datadetox.myshadow.org

Choose Privacy Week (US but useful) http://chooseprivacyweek.org/resources

Be aware of what you can do practically in your service.

Do your browsers keep a history of what your patrons have browsed?

If so what can you do about this? Talk to IT about a different browser that doesn't collect histories – change settings to stop collecting?

Do you offer any sessions explaining what google etc does with your data?

Tell users what you are doing with their data which they give you – raise awareness – be honest.

Opening up access to research outputs David Carr – Wellcome Trust

David spoke about the Wellcome Trust's approach to trying to ensure open access to not just traditional research outputs in the form of journal papers but also data sets, software, and other research materials resulting from Wellcome funded research.

This includes a partnership with several pharmaceutical companies to increase access to clinical trials data for those with a legitimate need to access.

Personal data versus transparency Malcolm Todd, National Archives

Malcolm noted that the 1998 act is still in law until Spring 2018 when a new Data Protection Bill based on GDPR will come into force. The principles are very similar to 1995 but the main changes are due to the increased use of technology to manage data and the increasing ease with which data can be used to do more and more things. Companies tend to find that they can do things with personal data and go ahead and do them without thinking about the implications.

Other changes include areas

- Children
- Digital services
- Consent
- "Right to be forgotten" actually should be "right to not be googled"
- Big data, social media, globalisation
-

Malcolm used an example from 2016 when companies house put forward a proposal that records of company directors would be deleted after 6 years rather than the current 20. This got quite far on the government approval process before journalists got hold of the story and raised a campaign. The government had to back down.

Again the clash between the individuals' rights versus the rights of the general public / country to be informed.

Forget versus remember

Malcolm challenged the current assumption of GDPR and similar regulation that less is always better in terms of personal data being stored. Thinking about what it is in the best interests of the data subject:

Is no data best? Probably never

Is minimal data best? Possibly but not always

How do we personalise the rules in some way to account for different situations?

GDPR may not last long!

Pervasive Internet Monitoring Slavka Bielhova, Open Rights Group

Slavka approached the topic from the point of view of LIS professionals who, in most cases, signed up to the profession with a view to enhance unrestricted access to information for patrons rather than to unrestricted monitoring of such use by the authorities.

It was the Edward Snowden whistleblowing report in 2016 which revealed that the NSA was intentionally spying on citizens of the US and wider afield. It became clear that the UK government was doing the same- possibly even more. However rather than any embarrassment the UK responded by bringing in the Investigatory Powers Act 2016 which simply legalised everything they had previously been doing illegally.

The act gave broad powers to the authorities to access datasets, hack telecommunications, order companies to build back-doors into their systems so that the government could easily break in, and order companies to release data about their clients use of their systems. What is more the companies are forbidden from disclosing that they have been asked to release the data or give access to their systems.

Obviously, this included LIS systems, datasets, records, etc.

A further law due soon will state that repeated viewing of terrorist content online will become a crime. But lack of clarity:

- Who decides what constitutes “terrorist material”
- How often in “repeated”
- What about historians, journalists, ect wanting to access.

As well as the government there are also companies accessing our data notably Google, Facebook etc.

What can LIS do? We have to abide by the law.

- Make sure we are not part of the problem. Is our service above people’s privacy?
- Get involved – educate our users
- Be proactive – advocates and spokespeople for the cause of privacy.

Big Data, Libraries and Privacy – Stephen Wyber, IFLA

Stephen's talk focused on big data and the flaws in the argument about anonymization.

He quoted examples where high 80% and 90% of so called anonymised data could be linked back to individuals by cross referencing with other sources.

He pointed out the hazards of correlation and causation.

The talk ended with an examination of codes of ethics of professional organisations and identifying the extent to which privacy was covered in these documents.