Data protection, public services and workers' rights

Appendix to EPSU Position Paper on Smart Public Services for a Digital Age, adopted by the EPSU Executive committee on 19 April 2016

Digitalisation poses a range of new opportunities as well as problems for both public service workers and the wider population who depend on those services. While a growing body of research has explored many of the issues relating to digitalisation and data protection, it has largely been from the perspective of business, government and service users. An extensive literature review on the subject commissioned by EPSU began to address this, but made no specific references to data protection, which remains a particularly under-examined feature of the digitalisation process. It did however discuss changes made in the draft 2012 European data privacy framework, replacing the 1995 Directive. It is therefore important to asses the challenges and opportunities that "once only" and "digital by default" policies along with the effects of upcoming trade agreements may have on data protection issues, and the consequences for public service workers.

Consequences include the increasingly comprehensive nature of document management systems which can be transparent for employers and not workers, an increasing fusion of work and private life associated with the official use of private work equipment such as mobile phones and laptops. As well as the monitoring and data mining of sites by employers to develop insights into workers private lives.

These issues have not gone totally unnoticed. During the "Arbeit 4.0" conference organized by Ver.di in June 2015, General Secretary Frank Bsirske called once again for the creation of an Employee Data Protection Act to strengthen the position of unions in dealing with these new issues, and to adequately protect the data security of workers.

What ought to be of concern here is both the danger of personal data being accessed or mined without someone's consent and the privatisation or marketisation of public data.

Implications of trade deals on data security

The Safe Harbour data agreement between the EU and US posed a serious threat to the data security of EU citizens, as it allowed data relating to EU citizens to be provided to U.S. companies who do not guarantee the same protections as in the EU. According to a ruling by the European Court of Justice, Safe Harbour "did not afford an adequate level of protection of personal data" (Arthur, 2015). Though many commentators believe that companies will find alternative means to evade the EU Data Protection Directive, despite this and other rulings. Negotiations are now ongoing to 'amend' the agreement so as to bring it in line with EU directives and guidelines on Data Protection. There remain, however, reasons for concern, after an EU "senior official" is reported to have stated at the EUs annual Transatlantic Conference that "[the EU is] on the same page as the US theoretically on the issue of data flows" (Flemming, 2015). Furthermore, the Commission working party responsible for protection of individuals with regard to data protection "is urgently calling on the EU Member States and the European institutions to open discussions with the US authorities in order to find a political, legal and technical solution that enables companies to

transfer personal data to the US" (Ahearn, 2015). The ruling then is clearly not final, and discussions are ongoing. Jan-Philipp Albrecht, a German Green/EFA MEP has also expressed serious concern that these core rights may still be negotiated away or watered down as part of ongoing discussions (Franke, 2015).
As of March 1st, negotiations resulted in the announcement of a "privacy shield" to protect EU citizens data[1], as a requirement for the implementation of a "Safe harbor 2.0". Despite minor improvements, it's been reported in a statement by Max Schrems, that "the Shield proposal lists six legitimate uses for bulk data collation" including "detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to US or allied armed forces; and combating transnational threats, including sanctions evasions" (Orlowski, 2016).

Aside from any potential issues resulting from this, TTIP itself certainly will include "investor-state provisions" which pose threats to employee data protection rights. The inclusion of "Investor-state provisions" means that if new regulation gets in the way of a U.S. (or any) investor's ability to make profit, they could be able to sue the country for monetary losses. Not only for losses on what they expected to gain as the result of a particular deal but also for "expected future profits". This would also require a new court system. As noted by the Electronic Frontier Foundation, "Since these supposed lost "investments" can even include intellectual property, big media companies could use ISDS to undermine data protection rights (Malcom and Sutton, 2014).

Most of the discussions relating to data protection refer mainly to the risks to business. However, as the 2012 Gartner's Security & Risk Management Summit it was noted that "Monitoring employee behavior in digital environments is on the rise […] with 60 percent of corporations expected to implement formal programs for monitoring external social media for security breaches and incidents" (Moore, 2015). The current law does not regard social media sites as 'private' spaces, regardless of security settings. The TUC also noted that "most tribunal cases result from a co-worker or manager printing off a Facebook entry they object to and sending it to HR" (TUC, 2016). It's also worth noting that several black holes in data security are developing in relation to in paper or material documentation (Siggers, 2016), which highlights the need for much greater legal clarity.

This means that employers are now able to read this information as a "public" asset anyway. This disparity between the personal nature of the content of social media, and it's status as a private, rather than accountable and public service, has lead for calls to "nationalize" Facebook. Especially as it has continuously failed to uphold decent data protection standards (Howard, 2016), but the implications of new trade agreements place further threats. Given that many private social media sites make their money from the use of private data, particularly in relation to marketing companies, its feasible that an ISDS (or any variation of this body) could be used to sue a country which attempts to prevent a such a company from using information in breach of data protection legislation.

Further to this, it's unclear whether or not public services which become outsourced can ever be re-municipalised. For example, if a water company was contracted to deal with a service generally provided by the local government, and could not guarantee the same level of data protection, would this constitute a sufficient legal basis for re-municipalisation, even if doing so would damage profits? This of course raises serious questions regarding the right for member states, and the citizens generally to maintain control of their data.

[1] http://europa.eu/rapid/press-release_IP-16-433_en.htm
http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

Privatisation

While there is a reasonable expectation that the Government will collect data in line with existing data protection legislation, the privatisation of certain Government functions may result in personal data being shared with private companies. The concepts of "once only" and "digital by default" coupled with the privatisation of certain government functions, pose a threat to employee data protection. 'Digital-by-default' is the idea that services should be delivered digitally as the primary (if not only) option. The once-only principle is the idea that a citizen should only have to provide information to public authorities only once, with this information then saved and shared between all levels of government. Records submitted to a particular government department could then be shared not only with all other departments but potentially also contracted private companies. In effect, employees and citizens may see their private data handed over to private companies without their direct consent.

Despite positive references to 'open data' made by the commission in regard to its ability to facilitate innovation, concerns arise. "Anonymous" big data, such as traffic or crime statistics for example, have already been made 'public' for use by private businesses or individuals in some cases. For example in Helsinki, where the Municipality's "open data" policy provides government statistics, such as traffic data to be made publically available for use by private businesses. This could lead to "back door" privatisation of personal data, and an undermining of data protection, but also poses issues about use.

The ability for private companies to "cannibalise" 'big data' can have other unintended consequences. The Chicago Police Department developed seemingly innocent algorithm which intended to mine big data to develop crime and risk assessments and assist with targeting resources more efficiently. However, it ended up being widely accused of discriminating against low-income, black neighborhoods and their inhabitants. The data that any algorithm mined is ultimately entered and interpreted by human beings (Kun, 2015) and this can quite easily become discriminatory, for example, Google algorithms replicate discriminatory patterns and views about certain groups of people as seen in Google algorithms regarding transgender people.

It's fair to assume that 'in house' public services would have a greater commitment to higher standards of data protection due to the values embodied within the sector. The threat of privatisation potentially increases these risks, as tackling unfortunate discriminatory side effects of seemingly 'neutral' algorithms will not be prioritised.

Conclusion

The dangers of allowing private companies to handle data are therefore far reaching, from "back door" privatisation and the potential slow erosion of data protection rights, to the risks of discrimination of big data mining. The overall discourse around this key subject has so far been framed largely in terms of risks and benefits to employers and Governments. EPSU opposes all trade agreements which endanger employees and citizens data protection rights, and will continue to fight for interests of workers and citizens in relation to data protection rights in all areas where these rights are threatened.

We believe that workers must be informed of what sorts of data their employer can legally have access to, where they will store it, and who it will be shared with. Furthermore we support the formation of an 'Employees Data Protection act' which could directly address and protect the rights of workers in the future.

References

- Ahearn, T. (2015). *US and EU Need Safe Harbor Solution by End of January 2016 to Avoid Enforcement Action - ESR News Blog*. [online] Esrcheck.com. Available at: http://www.esrcheck.com/wordpress/2015/10/20/us-and-eu-need-safe-harbor-solution-by-end-of-january-2016-to-avoid-enforcement-action/ [Accessed 1 Mar. 2016].
- Arthur, C. (2015). *'Safe harbour' ruling illustrates growing chasm between US and EU*. [online] the Guardian. Available at: http://www.theguardian.com/technology/2015/oct/06/safe-harbour-ruling-growing-chasm-us-eu-data-protection [Accessed 18 Feb. 2016].
- Boillat, P. and Kjaerum, M. (2014). *Handbook on European data protection law*. 1st ed. European Union Agency for Fundamental Rights.
- Brownlee, L. (2016). *Forbes Welcome*. [online] Forbes.com. Available at: http://www.forbes.com/sites/lisabrownlee/2016/01/22/eu-spokesperson-intense-negotiations-eu-us-safe-harbor-are-ongoing/#2db87532471a [Accessed 1 Mar. 2016].
- Flemming, J. (2015). *Brussels makes overture on 'data flow' agreement in TTIP – EurActiv.com*. [online] Euractiv.com. Available at: http://www.euractiv.com/section/trade-society/news/brussels-makes-overture-on-data-flow-agreement-in-ttip/ [Accessed 18 Feb. 2016].
- Franke, K. (2015). *TTIP and the right to protect personal data*. [online] openDemocracy. Available at: https://www.opendemocracy.net/can-europe-make-it/keno-franke/ttip-and-right-to-protect-personal-data [Accessed 25 Feb. 2016].
- Gibbs, S. (2015). *What is 'safe harbour' and why did the EUCJ just declare it invalid?*. [online] the Guardian. Available at: http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection [Accessed 23 Feb. 2016].
- Howard, P. (2016). *Why We Should Nationalize Facebook—Really*. [online] Slate Magazine. Available at: http://www.slate.com/articles/technology/future_tense/2012/08/facebook_should_be_nationalized_to_protect_user_rights_.single.html [Accessed 29 Feb. 2016].
- Kun, J. (2015). *Big data algorithms can discriminate, and it's not clear what to do about it*. [online] The Conversation. Available at: http://theconversation.com/big-data-algorithms-can-discriminate-and-its-not-clear-what-to-do-about-it-45849 [Accessed 4 Mar. 2016].
- Malcom, J. and Sutton, M. (2014). *EU-US Trade Negotiations Continue Shutting out the Public—When Will They Learn?*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2014/10/eu-us-trade-negotiations-continue-shutting-out-public-when-will-they-learn [Accessed 23 Feb. 2016].
- Moore, S. (2015). *Gartner Says Monitoring Employee Behavior in Digital Environments is Rising*. [online] Gartner.com. Available at: http://www.gartner.com/newsroom/id/2028215 [Accessed 25 Feb. 2016].
- Orlowski, A. (2016). *Safe Harbour v2.0 greenlights six bulk data collection excuses*. [online] Theregister.co.uk. Available at: http://www.theregister.co.uk/2016/03/01/safe_harbour_20_oks_six_bulk_collection_excuses/ [Accessed 1 Mar. 2016].
- Siggers, G. (2016). *People and paper: the well-intentioned threat of data protection and privacy?*. [online] Continuitycentral.com. Available at: http://www.continuitycentral.com/index.php/news/erm-news/880-people-and-paper-the-well-intentioned-threat-of-data-protection-and-privacy [Accessed 25 Feb. 2016].
- TUC, (2016). *Can my employer monitor what I'm writing on Facebook while I'm at work? | workSMART*. [online] Worksmart.org.uk. Available at: https://worksmart.org.uk/work-rights/discipline-and-policies/social-media/can-my-employer-monitor-what-i%E2%80%99m-writing-facebook [Accessed 25 Feb. 2016].