Cyber Law - Privacy at the Edges

15:15 - 16:45 Thursday, 3rd September, 2020
Track Cyber Law

---

164 Law Enforcement Access to Encrypted Data Across Borders

Jessica Shurson
Queen Mary University of London, London, United Kingdom

Abstract

This article explores the extent to which ‘technical capability notices’ issued pursuant to UK and Australian law, which allow law enforcement exceptional access to encrypted data, may have extraterritorial effect in light of the US Cloud Act. The Cloud Act came into force in April 2018 to facilitate foreign law enforcement access to data held by US service providers through the use of bilateral agreements premised on mutual trust. The first such agreement – the UK-US Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime – allows for UK law enforcement to send production orders, authorized under UK law, directly to the US service providers for communications and content data.

This recent UK-US agreement, and the announcement of negotiations for a similar agreement between Australia and the US, have led to confusion concerning whether technical capability notices—essentially, decryption orders—may be served on US service providers pursuant to these bilateral agreements, and whether these investigatory powers might be ‘imported’ to US law enforcement as well. This article will explore how the ‘encryption-neutral’ provision of the Cloud Act allows for the UK, and possibly Australia, to serve technical capability notices on US service providers extraterritorially. To reach this conclusion, the article will analyze the relevant provisions of UK and Australian law, how those provisions interact with bilateral agreements pursuant to the Cloud Act, and the likelihood of the enforcement of UK and Australian technical capability notices on US service providers. To the extent that these notices are enforceable extraterritorially, the article will conclude with an analysis of whether these UK and Australian investigatory powers are thus imported to US law enforcement.

189 THE TRADITIONAL CONCEPT OF HABEAS CORPUS AND MODERN DANGERS FOR PRIVACY THROUGH THE USE OF WEARABLE APPS

Elena Falletti
Università Carlo Cattaneo, Castellanza, Italy

Abstract

The aim of this abstract regards the analysis of privacy management of wearable devices (hereinafter “WD”) absorbing personal data from a user’s body and from his or her behavior. There are many discussions on privacy, and WD privacy management is only one of them, while the main one is about what privacy is. Indeed, there are different opinions on managing the most individual private information. On the one hand, some people affirm that privacy, in an age of invasive electronic communication, should be a fundamental right. On the other hand, other views support that privacy has to be treated as an additional service that the user can buy if markets are interested in it. Indeed, the strict contact between the user’s body and the wearable device may give the impression that privacy is a “plus” service included with the WD product.

Indeed, WD use represents a transformative concept of privacy, since processing the whole data pertaining to an individual involves the digital reconstruction of this person, and his/er physical and psychological characteristics. Habeas corpus represents the strong tradition of human dignity and human rights protection, and it could be a bridge between a legal institution of great historical tradition and modern needs in the field of personal data protection in the WD environment. It could overcome both American and European regulations limitations. Indeed, on the one hand the U. S. regulation seems focused exclusively on patent protection and consumer matters, and on the other hand, the E. U. discipline seems to have a very formalistic and bureaucratic approach. In both cases, rules do not seem to be sufficiently adequate. Rather, through this legal entity it seems to be possible to maintain high parameters of protection of individuality and to ensure the most intimate aspects of personal expression.

214 The Internet of Personalised Things. IoT-Powered Consumer Manipulation as an Unfair Commercial Practice

Guido Noto La Diega
University of Stirling, Stirling, United Kingdom

Abstract

Personalisation is one of the key befits of the Internet of Things (IoT). IoT traders can combine data from multiple sources and access consumers' most private spaces. At the same time, these traders retain control over their smart devices ('Things') throughout their lifecycles. Thanks to this combination of deep knowledge of the consumer and control over the Thing, IoT traders can personalise products, services, prices, and even the terms of service that regulation the business-to-consumer relationship. The problem is that personalisation can lead to consumer manipulation and even discrimination – such detrimental effects can be referred to as the 'Internet of Personalised Things'. Situational data and information about consumers' biases and vulnerabilities allow IoT traders to influence consumers' decision-making in surreptitious ways. This can go from instilling the desire to purchase useless or even dangerous Things, to the exclusion of BAME people from certain job ads, through to electoral manipulation. This paper critically assesses whether unfair trading laws – and in particular the Unfair Commercial Practices Directive as amended in 2020 – are fit for purpose and can provide a successful strategy to re-empower consumers, thus re-building trust in the IoT. It is suggested that, despite some shortcomings, this regime can be invoked by consumer to counter IoT-powered manipulation, especially as the Directive provides special protections for vulnerable consumers and against traders' undue influence impairing consumer freedom of choice. The Directive does have some limitations but this should not come as a surprise. Being a neoliberal instrument aimed at pursuing a perfectly competitive single market, it cannot provide an entirely satisfactory response to an issue that capitalism itself created, namely the problem of manipulated needs as discovered by Marx.

282 Law and the Costs of Connection: Social Theory, Privacy and Speech

Andrew Kenyon
University of Melbourne, Melbourne, Australia

Abstract

Among many analyses of contemporary networked communications and society, the work of Nick Couldry and Ulises Mejias offers interesting material for law. Their 2019 book, *The Costs of Connection*, is a notable recent work in critical internet studies and social theory that argues human life itself is being colonised by data. *The Costs of Connection* argues a new social order is emerging through these changes, in which 'continuous monitoring and surveillance … undermine[s] the autonomy of human life in a fundamental way that threatens the very basis of freedom'. The focus is far wider than media (although Couldry has long been a leading voice in media studies) and it is not limited to democratic contexts, with the importance of China clear throughout the analysis. But the work also makes quite some use of research in law and related work in philosophy, which suggests it warrants engagement from legal scholars. To that end, the paper proceeds through three parts. What do Couldry and Mejias say in summary? What do they say about legal research, which they approach particularly through the lens of privacy, and to which I would add points about free speech? And what does that suggest as further ways to explore law's relevance to the social order they argue is emerging. Their work is, in many ways, a perceptive and engaging use of legal scholarship from outside law, but one which illuminates challenges for law and legal analysis.