pdp JOURNALS

ISSN 2049-5307

Privacy & Data Protection

Volume 19, Issue 1 October / November 2018

Headlines

- ICO prosecution results in a first-ever prison sentence, p.18
- First GDPR fine issued, and it's pretty modest, p.19
- CNIL publishes useful assessment on blockchain, p.20

Contents

Commissioner: "I'm at a crossroads now"

The UK Information Commissioner has reported to Parliament on her Office's investigation into personal data misuse by various parties during election campaigns.

The investigation, which is the ICO's largest ever, has garnered much attention this year since the Cambridge Analytica debacle emerged in March. The issues discussed in the report are either ongoing or require further action.

Introducing the report, the Commissioner, Elizabeth Denham, said that "throughout our enquiries we found a disturbing disregard for voters' personal privacy by players across the political campaigning eco-system — from data companies and data brokers to social media platforms, campaign groups and political parties."

In reference perhaps to her recent fine of Facebook (£500,000), and notices of intent to fine campaign group Leave.EU and insurance company Elden insurance (£135,000), the Commissioner stated "where there have been breaches of the law, we have acted. We have issued… enforcement notices that compel companies and campaigns to comply with the law. We've instigated criminal proceedings against SCL Elections Ltd and referred issues to other regulators and law enforcement agencies. And where we have found no evidence of illegalities, we have shared those findings openly too."

But the Commissioner likened her position now to being "at a crossroads", saying "trust and confidence in the integrity of our democratic processes risks being disrupted because the average person

(Continued on page 17)

"Look beyond passwords", says ICO

Online service providers should consider alternatives to passwords to keep their systems secure and meet their GDPR obligations, the UK's Information Commissioner's Office has said.

In new guidance on encryption and passwords, the ICO advises that "before designing and implementing a new password system, you should consider whether it is necessary to do so, or whether there is a better alternative that can provide secure access."

The guidance identified one common alternative for organisations to designing and implementing their own solutions as being to utilise a single sign on system ('SSO'). A SSO is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications.

While this has its advantages — for example a reduction in the number of passwords that a user has to remember — organisations must ensure that they are happy with the level of security that is offered by that system. They must also consider what will happen if the SSO is compromised, as this will most likely also result in a user's accounts being compromised.

(Continued on page 17)