BIZCOMMUNITY

GDPR: ground zero for a more trusted, secure internet

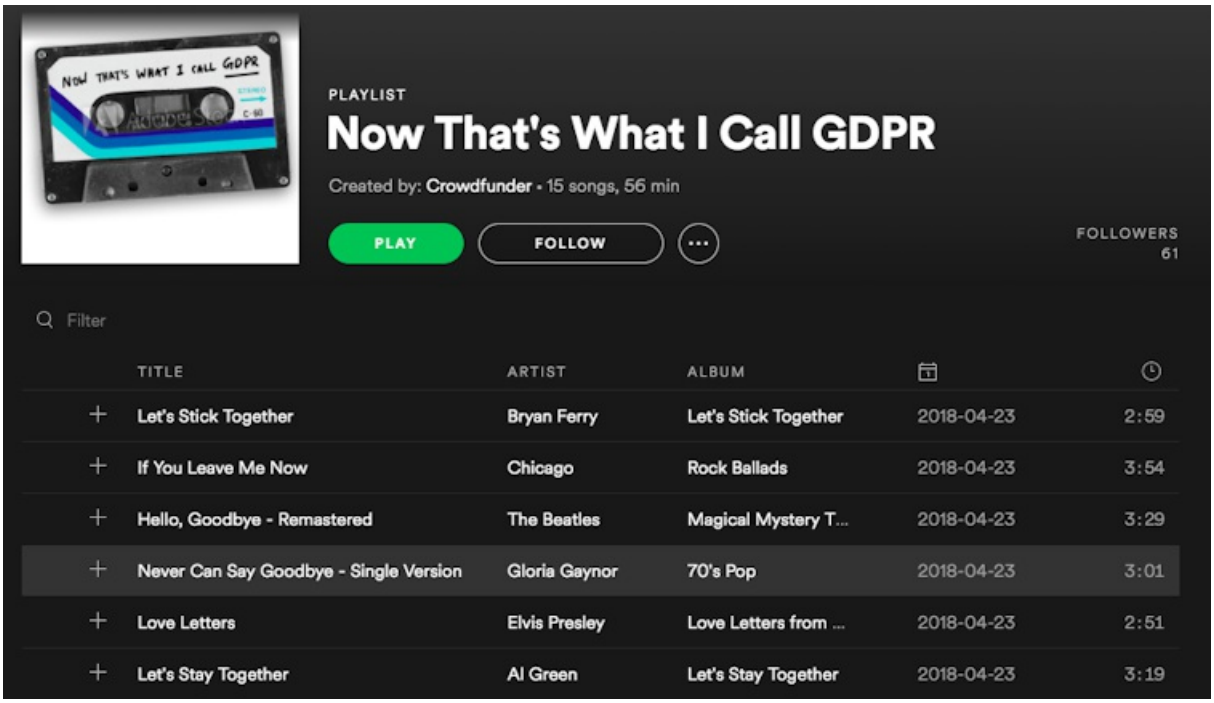
By Bill Buchanan

28 May 2018

Most of us have been bombarded recently by a barrage of emails from companies begging us to "stay in touch" or "opt in" or informing us of a "policy update". On May 25, an historic date for the internet, the EU's General Data Protection Regulation (GDPR) came into force. For some, it is the start of a more citizen-focused world, for others it will see the collapse of their digital marketing strategy.

Shutterstock

The number and scope of serious data breaches have dramatically increased in the last few years. In 2013, around three billion Yahoo user accounts were affected by a hacking attack. Recently it was revealed that 143m customers of the credit score agency Equifax were hit by a similar breach. And on top of this, we see breaches of privacy in the mass harvesting of data from Cloud service providers, as highlighted by the Facebook/Cambridge Analytica debacle. No wonder there is an increasing lack of trust in how companies capture and process our data.



Even Spotify has got in on the GDPR action. Spotify

A new dawn

GDPR replaces the EU's 1995 Data Protection Directive, which set out minimum standards for processing data. With the new regulations, individuals are afforded the power to compel companies to reveal (or delete) any personal data they hold, and failure to adhere to the new rules will result in stiff penalties, with a maximum fine of 4% of a company's turnover. For a company like Facebook, this could mean around US$1.6 billion.

Many companies already work within audit/compliance regimes. In the finance industry, for example, this is typically the Payment Card Industry Data Security Standard (PCI-DSS). But these regulations have often failed to stem the tide of data breaches within companies, necessitating more robust standards. At the core of GDPR there are four foundation elements:

Consent and how your data is used

As GDPR ensures that consent is explicit, the days of consent by default are over, and the need for users to opt out of mailing lists will become a thing of the past. Individuals have the right to withhold consent, request access to their personal information or delete it altogether from a site. Currently the general feeling is that few users are actually following up on the consent request emails, which means companies may experience problems with their current digital marketing strategies, as they see their contact lists collapse.

Response to breaches

In the past, companies have failed to respond promptly to data breaches, especially in the time taken to inform users, and are guilty of being vague about what they report. GDPR aims to overcome this by forcing companies to report within 72 hours, and have faster methods of investigating a breach. This is likely to see the rise of 24/7 security operation centres (SOCs) which continually monitor the data infrastructure for signs of a breach. With the current average time to detect a data breach measured in months, this will be a significant challenge for many companies.

Some of the focus areas of GDPR. Author Provided

Encryption

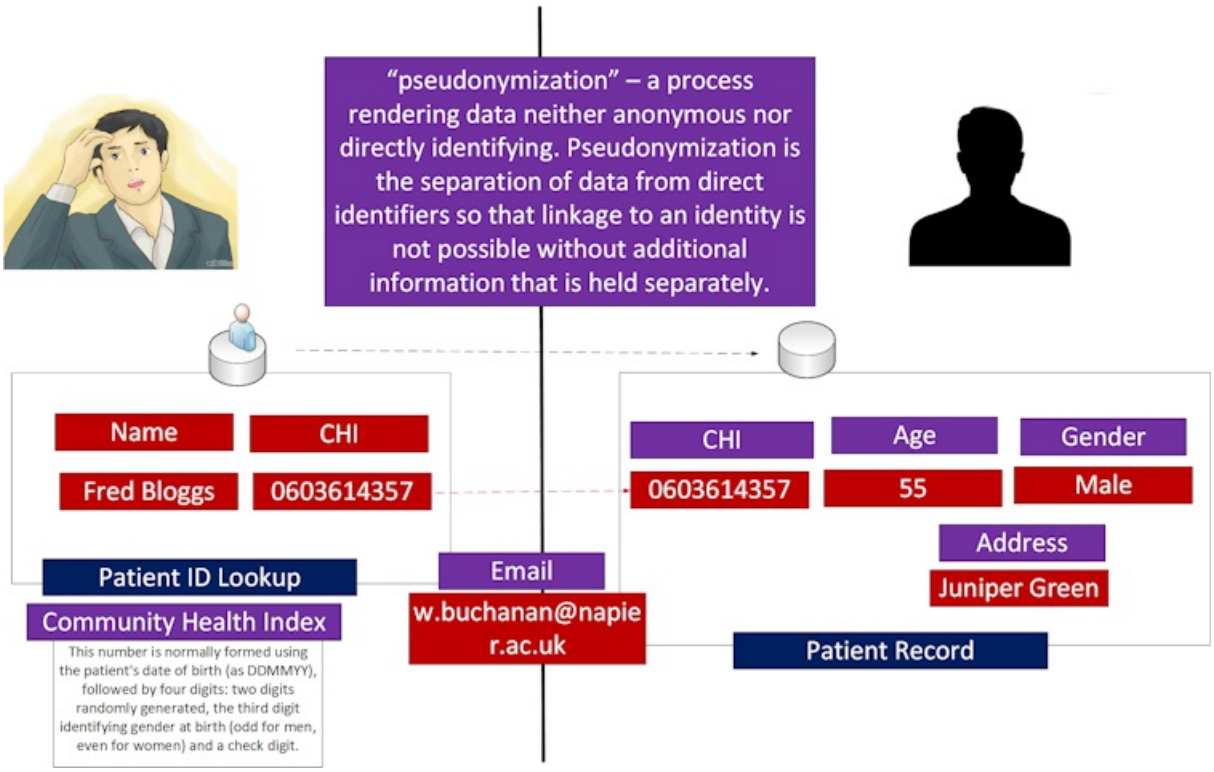
The real wake-up call for new regulation is that much of the internet is not trusted by users, who are concerned it does not embed security properly. Data must now be protected within encryption – encoding information so that it can only be accessed by an authorised user – wherever it relates to personally sensitive data. Companies must understand the scope of a data breach in terms of the information that can be extracted from a leak. If the data is encrypted, it will make it much more difficult to reveal the information.

In the past, the industry has generally struggled to implement encryption and rights protection on documents, but GDPR will force a move towards encryption by default and demand tighter controls on devices that access sensitive documents. The recent moves by Google and Microsoft to lock down their email systems with improved security sees some of the first proper attempts to integrate encryption and access control into documents accessed over the Cloud.

Protecting your privacy

Under GDPR, a particular challenge for many companies will be the separation of personally identifiable information (PII) – name, date of birth, phone number – from other elements of data. If we take the example of health records, a patient's community health index number (CHI) will be stored under a "pseudo-anonymiser" – an identifier that disguises the connection between someone's identity and their information.

This involves not just electronic separation on different databases, but physical separation on different systems. The merging of this information must then take place on a different system, and one that is highly trusted. But many see the concept of pseudo-anonymisation as weak from a privacy point of view, as details can often be mapped back to a particular ID if additional information is known.



The pseudo-anonymiser process.

So will we see an improvement in our online world in terms of protection and security? Well, definitely some, though many of the changes will happen behind the scenes with improved processes and security methods. But what we should notice is companies taking computer security more seriously. We should see simpler terms and conditions, better reporting on data breaches and companies demonstrating a more reassuring and responsible attitude to our data.

GDPR moves us truly into a more equal information age, where we are finally moving away from the weaker legacy systems of the past to build a more trusted, secure and resilient internet for the future.

This article was originally published on The Conversation. Read the original article.

ABOUT THE AUTHOR

Bill Buchanan OBE, Head, The Cyber Academy, *Edinburgh Napier University*