Clayden Law, Prama House 267 Banbury Road, Oxford OX2 7HT
E: info@claydenlaw.co.uk | T: 01865 339640

CYBERSECURITY SERIES: ENCRYPTION AS A PRIVACY TOOL

Encryption offers both security and privacy – in fact, it plays a key role in protecting an organisation's digital assets and the data held on behalf of its stakeholders.

Elizabeth Denham, the current Information Commissioner at the UK Information Commissioner's Office (ICO), has confirmed that the UK is going to implement the *General Data Protection Regulation* (GDPR) with effect from May 25th 2018, irrespective of the Brexit decision.

The GDPR introduces significantly more obligations upon organisations that handle personal data, and raises potential fines for cybersecurity breaches to an eye-watering €20 million or 4% of global turnover, whichever is greater. Among other obligations, the GDPR also introduces new requirements that require organisations to be more proactive in maintaining their own record keeping of privacy compliance, data privacy by design and default and data portability.

Taken together with the almost weekly news regarding serious data breaches, such as the record £400,000 fining of TalkTalk for its 2015 cybersecurity breach, it makes sense to review and adapt organisational privacy compliance to the requirements of the GDPR by May 2018.

Encryption is a powerful security tool. The ICO sees it as an *elementary* precaution for protecting personal data, meaning that it ought to be in the cybersecurity armoury of all personal data handling organisations.

All security measures have their strengths and weaknesses and none offers a panacea for cybersecurity. However, as there are clear links between the failure to encrypt data and enforcement action taken by the ICO, it is important to employ this technology.

While regulatory sanctions may well incentivise the use of encryption, they are just one of the many issues that may impact organisations in the event of a cybersecurity breach, such as reputation damage and intellectual property loss.

With that in mind, we have prepared an overview of what encryption does, why it is useful for privacy, and what problems it can solve (and some that it cannot).

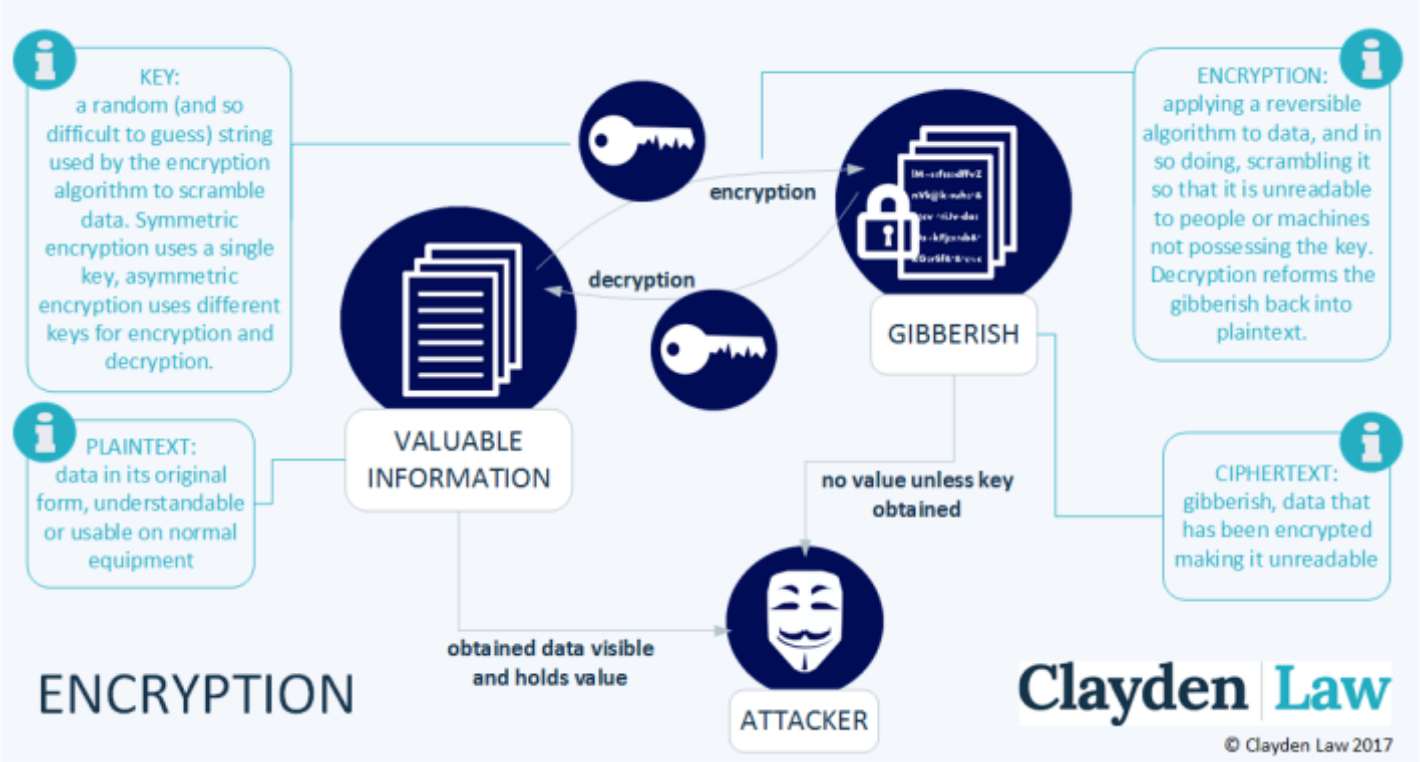
WHAT IS ENCRYPTION?

Encryption performed correctly, results in data that is in fact not data at all. To anyone without the secret *key*, it is incomprehensible gibberish. With the key, encryption allows valuable information to be converted into gibberish and reformed as needed.

First off, encryption is not to be confused with *hashing*, which irreversibly turns data into gibberish.

We use encryption for privacy protection as well as security because it reduces risks to the *confidentiality* of data. It serves as the last line of defence when, for example: an attacker has surpassed all existing layers of security; an employee has unwittingly allowed a personal data breach by misplacing their laptop on a train; or a web hosting provider has not patched their servers following the release of an essential security patch.

CONFIDENTIALITY:
"The property that information is not made available or disclosed to unauthorized individuals, entities, or processes"
ISO 27000:2016



From the ICO's perspective, it will look to take enforcement action against organisations who have:

- Failed to encrypt ***data at rest***, i.e. data that is being stored (for example on a hard drive or a USB stick)*;*
- *mismanaged* or misconfigured their encryption, making it ineffective (i.e. an attacker can easily get the key); or
- have used *obsolete* or *particularly weak* encryption methods.

As well as ensuring the privacy of individuals interacting with organisations that collect their data, encryption also supports confidentiality in business-to-business interactions. The value of concealing data from an organisation's competitors is also factor to consider when analysing the benefits of introducing or updating encryption technologies.

STRONG VERSUS WEAK ENCRYPTION

It is not enough for an organisation to say it is encrypting data - there needs to be some quality control, which is why it is common to hear people discussing *strong* or *weak encryption*.

No commercially available encryption is completely *uncrackable*. The maths geeks know *in theory* how to do it, but the computer geeks have not worked out how to generate the truly random numbers needed to facilitate it.

Strong and *weak* relate to how long a cryptanalyst (a person trying to decode what leaked encrypted data actually says) has to spend guessing before they work out what the data says or find the encryption key. In the absence of perfect encryption, ensuring that it would take millennia for a cryptanalyst with the latest technology to decrypt data has to be good enough. The less time it will take, the weaker the encryption, making strong encryption is industry best practice.

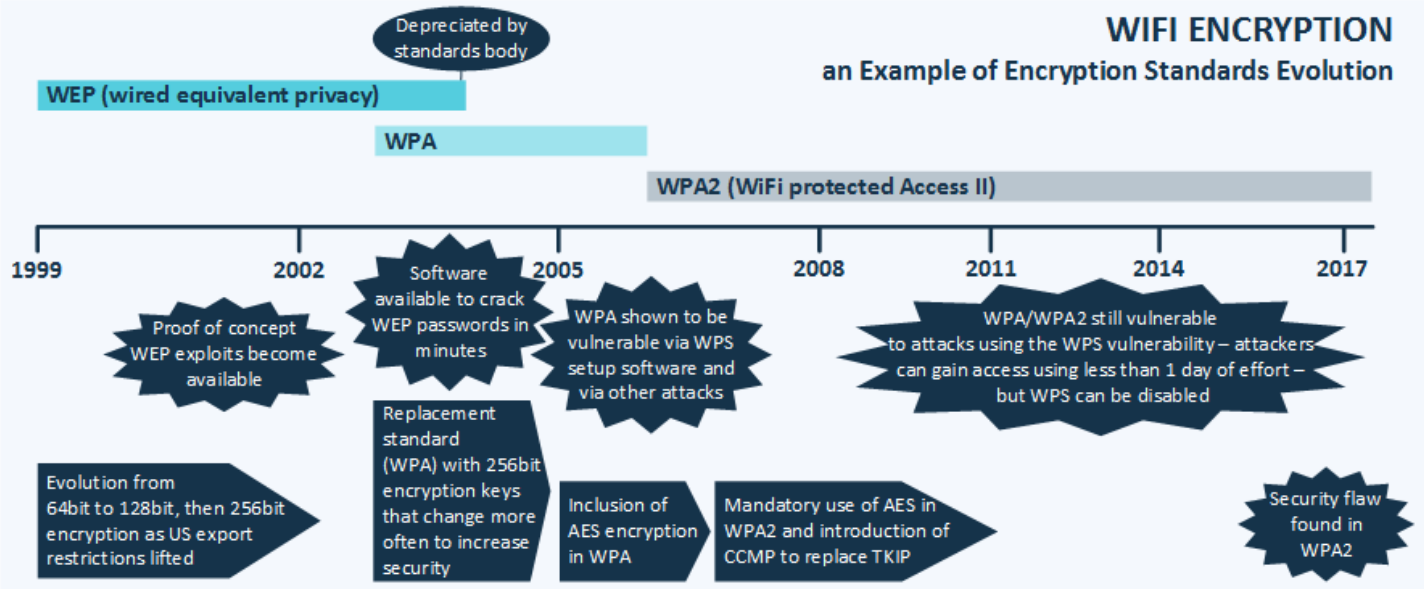
Clayden Law, Prama House 267 Banbury Road, Oxford OX2 7HT
E: info@claydenlaw.co.uk | T: 01865 339640

Encryption algorithms lose their strength over time. The algorithms themselves do not change, but the environment we use them in does. Computers get faster, parallel processing in the cloud gets cheaper and researchers constantly search for faults in each algorithm.

This is addition to an evolution of security responsibilities under the law – organisations do not operate in a static environment and they need to adapt to threats. Risk assessment is an important factor, necessary for GDPR compliance (and in a future article in this series, we will look more closely at what "risk" actually means in a cybersecurity context).

Due to concerns of encryption being used to enable secret communications by terrorists, both the UK and the US have explored allowing "backdoors" to encryption in recent years and early versions of the UK Investigatory Powers Bill (now the Investigatory Powers Act 2016) included such provisions. Due to concerns voiced by prominent cryptanalysts they were subsequently removed, however, the power of encryption for enabling harm remains of concern to the UK government and the security services.

Any encryption method that is worth having will have been subjected to rigorous testing by the community of cryptanalyst researchers. The general principle is the more researchers there are trying (and failing) to break encryption the more likely it is to be strong. If a vendor promises to be able to provide strong *proprietary* encryption, then one ought to be sceptical.



SYMMETRIC VERSUS ASYMMETRIC ENCRYPTION

Two further words often heard in association with encryption are *symmetric* and *asymmetric*.

In symmetric key encryption both encryption and decryption processes use the same secret key. This is great if only one person uses the data, or the people sharing data know each other and have shared the key before they begin to share encrypted data. This is frequently the type of encryption applied to *data at rest*.

In practice, we need to share information securely with people we do not know, with very little delay, across the Internet. As well as protecting data held on servers, encryption is the way that we create 'tunnels' across the internet so that our communications are private. We do not have the time to meet

the person, verify that we trust them and swap keys, so asymmetric (also known as *public key*) encryption allows us to communicate securely with strangers, including credit card companies, shops and customers. Asymmetric encryption is often referred to as being applied to *data in transit*.

Asymmetric key encryption uses two separate keys to encrypt and decrypt the data. The encryption process uses a *public* key, meaning that this key is not a secret. The person who wants to begin communicating can find and use this key without knowing the other person. Trusted organisations hold libraries of people's public keys, so we can check that we're encrypting something that only our intended recipient can read.

Only the recipient has access to the second, *private* key, which they use to decrypt the data.

ENCRYPTION UNDER THE DATA PROTECTION ACT AND THE GDPR:

Data Protection Act 1998
Principle 7 of the data protection principles under the Data Protection Act requires organisation to "*Appropriate technical…measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*"

The GDPR
From 25th May 2018, the GDPR (the General Data Protection Regulation), under Article 32(1)(a) will require that "*…the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including … as appropriate: (a) the … encryption of personal data;*".

THE LIMITATIONS OF ENCRYPTION

Encryption gets weaker over time as computers get faster, but cryptanalysts also find flaws that are more significant in encryption algorithms – sometimes something will happen that means that an urgent update, or even a change of encryption is needed.

Think of cryptanalysis along the lines of a detective drama – a crime is committed and initially everybody is a suspect. The detective's next step is eliminating large groups of people using evidence at hand e.g. maybe they were too far away to have committed the crime, or the DNA says they are looking for a woman and therefore all men can be eliminated. Eventually the detective gets to a point where there are so few suspects that it can start teasing out most likely culprit.

Sometimes a cryptanalyst can eliminate whole categories of encryption keys because of some quirk in the way the algorithm works (WEP), or there is a problem with the way the software was written (Heartbleed[1]), or it is so user-unfriendly that people make mistakes that cryptanalysts can use (that's what the scene in the pub in the Imitation Game[2] is about…). All of these things mean that it is worth holding onto your gibberish with a range of other security measures, just in case.

Also, as they say, "*there is no point having a bulletproof door in a chain-link fence*". Many of the organisations the ICO has taken action against thought that they were encrypting the right things in the right way. Unfortunately, they had either failed to do some other really basic security thing (leaving the attacker an easy way in), or the people implementing the encryption and failed to understand something important (like not storing the key in the same place as the encrypted data).

Encryption is a powerful tool, but it is easy to make a series of small mistakes that make it completely ineffective. It is not just about buying encryption software it is about installing it correctly, configuring

[1] heartbleed.com
[2] en.wikipedia.org/wiki/The_Imitation_Game

Clayden Law, Prama House 267 Banbury Road, Oxford OX2 7HT
E: info@claydenlaw.co.uk | T: 01865 339640

it to scramble the right data and undertaking a broader risk assessment that highlights other risks to reduce in parallel.

ENCRYPTION IN THE WRONG HANDS…

The GDPR requires those organisations holding data to make sure it remains accurate and can be made available to the data subject when they ask for it. These are the other two key concepts of cybersecurity – *integrity* and *availability*. Encryption will ensure confidentiality but it will not stop an attacker from corrupting data or making it unavailable to you. The most concerning version of this is ransomware, which uses encryption against its victims…

Ransomware is becoming a more significant threat, as attackers have increased access to the same strong encryption, meaning that companies entirely lose access to their data as it turns to gibberish before their eyes. This type of malware is also getting smarter, persisting in systems for enough time to locate networked backups and shared drives to reduce the chances that companies can protect themselves by having redundant copies.

Even if the data was encrypted before the attack occurs, the affected organisation will *still* have to report the personal data breach under the GDPR, because the data can't be made available to its subject.

ROUNDING UP

Encryption is a tool that, when used appropriately, can greatly mitigate the risk of breaching data protection law. This is even more the case under the new GDPR where it is formally recognised for the first time in the text.

The natural question is: if encryption is so effective, then why don't we encrypt everything?

The short answer is that even a computer's time costs money… Encryption adds a delay to any communication or makes a computer work harder when it is saving/retrieving files. That means that this processing time and bandwidth cannot be used for other business requirements.

Any delay caused by encryption may be the tipping-point between a system working and being unacceptably slow. High-bandwidth or low-confidentiality services might choose to prioritise speed over security – security is all about balancing risk appetite against providing a service to users. In the case of encryption, this leads to a dilemma – how far can we protect privacy while allowing people to interact freely?

Organisations controlling or processing data in the EU and elsewhere need to make privacy and cyber security decisions with considerable care. Practically speaking, once an organisation determines the risk of processing data, it will be in a better position to argue its decision as to the use, frequency and type of encryption employed.