Digital gold

Andrew Hogan looks at the legal implications of the trade in personal data

At the time of writing, the price of oil and other carbon-based fuels is soaring. Oil has long been a precious resource, for well over a century being the commodity upon which any industrial economy has been built. But carbon-based fuels are set to pass into history in the coming decades, rendered obsolescent by concerns about climate change and energy security.

Perhaps now the most valuable commodity in the world is information. In the 21st century, pieces of data - placed in the correct context and disseminated to the right user for whom they have a particular value despite having no material weight or tangible presence - can be transmuted into money with an ease that the seekers of the philosophers' stone could only dream about.

In the legal field, one example of this phenomenon is the trade in personal data of those who have a valuable cause of action at law, to those who can monetise that cause of action into a settlement of damages and costs.

Anodyne contact details consisting of names, addresses, emails and above all telephone numbers, which identify someone who potentially has a valuable cause of action because they have been involved in an accident, or purchased a PPI policy, or imprudently bought a timeshare or opted out of their final pension scheme, are a valuable commodity, which is apt to be bought and sold like any other.

REGULATION

The trade in this information is not unfettered by regulation. The individuals concerned have an interest in their data, and an interest in maintaining their privacy. Often both those interests may be infringed, by the sale or transmission without their consent of their data; and a consequent intrusion into their privacy by incessant telephone calls or texts by claims management companies seeking to secure business.

Sets of personal data of this nature are not usually gathered in isolation, but are collected into a database, which can function as a marketing list. Databases are a protected class of property under the Copyright and Rights in Databases Regulations 1997. This facilitates the sale of the database as a valuable piece of property.

Under these regulations, a 'database right' will be created for the benefit of the creator of the database if there has been a substantial investment in obtaining, verifying, or presenting its contents. If, without the consent of the owner of the right, someone else extracts or re-uses all or a substantial part of the contents of the database, they will infringe the right, and an action may follow, in addition to any action for breach of confidence.

However, the contents of the database must be lawfully obtained, and regard had to the Data Protection Act 2018 and the UK-GDPR, which apply to protect the interests of data subjects, whose details may otherwise form part of a valuable database. In this respect to process personal data, there must be a valid lawful basis for doing so.

There are six available lawful bases for processing someone's personal data: they include contract where processing is necessary to deliver a contractual service to the subject; a legal obligation to process someone's personal data, where vital interests are at stake requiring processing; where there is a public task requiring the processing; where there is a legitimate interest in the processing; and where someone consents to the use of their data. It is this last category on which use and sale of data will usually be based.

The Information Commissioner's Office has emphasised the following guidance on obtaining consent:

- Consent requires a positive opt-in. Do not use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.

● Keep your consent requests separate from other terms and conditions.
● Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
● Be clear and concise.
● Name any third-party controllers who will rely on the consent.
● Make it easy for people to withdraw consent and tell them how.
● Keep evidence of consent – who, when, how, and what you told people.

Often claims management companies (and solicitors who buy leads from them) will assume or be assured that consent has been obtained. But this will often not be the case. Consent may have been given in the dim and distant past by a consumer to some processing of their personal data, but it is a big leap to then assume that this will permit sale of the data to an unspecified third party for a collateral purpose.

USE OF THE DATA

It follows that without consent having been obtained, and capable of being evidenced, a database that may apparently be the key to unlocking many thousands or even millions of pounds in claims may be incapable of being used. Worse, it may have been unlawfully compiled, and render the possessor of the database a target for litigation. Lawfully obtaining the data is only part of the picture, however. The purpose of getting the data is to use it, and in practical terms that means making contact with the individuals who have a valuable right to compensation for some sort of claim that the claims management company or other database holder wish to monetise. In the digital age, this practically means using electronic means to contact someone.

Actual use of the data and marketing activities using the data is largely governed by the Privacy and Electronic Communications (EC Directive) Regulations 2003. These regulations complement the general data protection regime and give more specific rights regarding electronic communications including telephone calls. The regulations have been amended on several occasions, including most notably in 2018 to ban cold calling in respect of claims management services and in 2019 to amend the definition of consent. The regulations include within their scope marketing by phone, email, text, or fax, and using cookies on a website.

In the leadup to claims management regulation passing from the Ministry of Justice to the Financial Conduct Authority (FCA) on 1 April 2019, the FCA set out what its likely approach will be to the acquisition, handling and use of personal data by claims management companies, in a paper called *Claims management-how we propose to regulate claims management companies*.

Cold calling and nuisance texts are noted as a particular problem, and among the measures proposed is a requirement for CMCs to retain recordings of telephone calls and copies of messages for a defined period:

'4.10 In line with the Brady Review's recommendation, we propose to require CMCs to record all calls and electronic communications such as text messages and e-mails with all their customers and potential customers. We propose that CMCs will need to keep call recordings for a minimum of 12 months after the latest of:
● the CMC's final contact with the customer
● the conclusion of the contract with the customer
● the settlement of the claim
● the decision by the customer to no longer pursue the claim or the withdrawal of the claim by the customer
● any related ongoing legal proceedings have finished
● the conclusion of the handling of any complaint made by the customer to or about the CMC

'4.11 A recording of a sales call to a customer which does not result in any further contact will therefore need to be kept for 12 months.

'4.12 CMCs carry out a large amount of business by telephone; so this is where much of the harm in the market happens. For example, harms resulting from misleading or aggressive sales or marketing techniques, and cold calling. So we consider it appropriate to require CMCs to record all customer calls about the claim, from advising a customer about the claim to conversations giving information and updates. It would also apply whether the CMC or the customer makes the call.

'4.13 Among other benefits, this will help us to identify if a CMC is not complying with the prohibition on cold calling without consent. Having this information means we will be able to work with the relevant authorities to identify and act on poor practices.

'4.14 CMCs would not have to record communications with third parties (eg. financial services providers) under these new requirements.'

It will be readily apparent that the FCA's putative requirements indicate that a huge amount of data will itself have to be retained for any rolling 12-month period, in effect to provide a rolling body of work that can be audited or used evidentially where a complaint is made.

But in a sense that is one of the least onerous of the requirements, because the FCA has also indicated that it wants to see a step change in due diligence regarding the acquisition of leads:

'4.8 We propose that CMCs should undertake due diligence on any lead generator from whom they accept leads. For example, the CMC should check that the lead generator is authorised (or is entitled not to be authorised) and has processes in place to ensure leads are obtained in line with relevant data protection legislation and privacy and electronic communications legislation which includes the government cold calling ban. We propose that CMCs must not use a lead generator if the CMC is not satisfied about the systems and processes in place for that lead generator. CMCs will also need to keep a record of the source of any leads.

'4.9 CMCs that get leads from third parties based overseas must also ensure that the third parties have followed the relevant requirements. Generally, leads from third parties based in the UK or outside the EEA must have been acquired in line with UK requirements. Leads from third parties within the EEA (except the UK) need to be acquired in line with the requirements set down by that EEA state.'

This requires positive vetting: sampling, auditing, and other practices to show that the data is lawfully acquired. Solicitors firms would prudently adopt the same approach, even though their primary regulator is the Solicitors' Regulation Authority.

One of the ironic consequences of a tougher approach to regulation is that the claims management companies themselves may find that they become targets for data breach litigation, in the post GDPR world, which might form a useful supplement to enforcement action by the regulators - and bring an end to the practice of annoying telephone calls from Manchester asking quizzically as to whether you have had an accident in the last three years.

Andrew Hogan practices from Kings Chambers in Manchester, Leeds and Birmingham. His blog on costs and litigation funding can be found at www.costsbarrister.co.uk