CLIFFORD
CHANCE

FACEBOOK, DATA MISUSE AND WHY IT MATTERS

— THOUGHT LEADERSHIP

MAY 2018

FACEBOOK, DATA MISUSE AND WHY IT MATTERS

As every news cycle brings further revelations about the alleged misuse of personal data by social media companies and political consultants, regulators, politicians and the public are more concerned than ever with what happens to information placed online, who has it and how it is being used.

Data protection and other enforcement authorities and politicians have significant powers to conduct investigations and take action, whether by imposing penalties or restrictions or by requiring senior executives to provide answers. As recent events have shown, the mere fact of their embarking on doing so can have immediate and severe commercial consequences. In serious cases such as this, the costs of investigations are far exceeded by the much longer lasting damage to the share prices and reputations of organisations involved.

The current press furore will subside. Lessons will be learned about how organisations should react to the reputational crises that arise from allegations about data security and usage. However, issues relating to data security and misuse will remain high on regulators' and politicians' agendas worldwide for some time. It is likely that attention will soon turn to the collection, use and analysis of data by a much wider range of businesses than those at the centre of current allegations. Increased public and political awareness is likely to translate into sustained levels of enforcement activity by multiple regulators and potentially protracted litigation in multiple jurisdictions.

Considerable uncertainty about approaches and priorities of regulators and of courts remains as the legal systems of countries around the world race to catch up with rapid technological advances. However, it is possible to put in place plans to minimise the extent to which misuse may occur and to respond appropriately if it does. The current inquiries may provide a guide to the areas which businesses making and updating such plans should prioritise when seeking to identify and mitigate the risks associated with the ways in which they use and share data.

Key issues

- The boundaries of what individuals may have consented to when placing their own data online are typically not clear, but imminent changes under the EU General Data Protection Regulation (GDPR) will impose stronger requirements for businesses to tell individuals how they will use and share data and to ensure that they have individuals' clear and informed consent.
- GDPR will also strengthen individuals' rights to know what has happened to their online data and to insist on its deletion. Substantial practical challenges will follow for businesses as individuals react to allegations that their data may have been misused.
- Significant litigation is likely to arise from allegations of data misuse. Potential claimants have numerous means by which they may seek compensation in various jurisdictions.
- Current investigations may only be the start of the process. All organisations which use and transfer customers' data should be ready for enforcement agencies, politicians and the public to closely scrutinise their data protection arrangements.
- Businesses need to develop and maintain tailored plans not only to minimise the prospect of data misuse, but also to respond quickly and effectively to suggestions of wrongdoing.

The allegations

Cambridge Analytica (CA) is alleged to have misused personal information from the Facebook profiles of approximately 87 million US voters without their authorisation. The information included names, locations, email addresses and details of "likes". It was gathered through a personality app accessed through Facebook by approximately 270,000 individuals. Their data and that of their Facebook friends was then used to build a system that could target them with personalised political advertisements during the 2016 US presidential election. Some press reports allege that the same conduct has been replicated in polls in other countries.

Facebook's platform policy at that time allowed friends' data to be used, but only for the purpose of improving the Facebook user experience. The policy stipulated that information was not to be sold or used for advertising. Facebook is alleged to have become aware in 2015 that individuals' data were being used in this way, but to have failed to tell users about how the information was being used and to have taken only limited steps to recover or secure the information of those affected. Facebook has claimed that no data breach occurred, but rather that CA improperly received and used the data against its terms of service.

Who owns individuals' online data?

Individuals' online data belong to them. Social media companies generally make it clear in their terms of service that individuals own all of the content and information posted on their networks and control how that information is then shared. The individual also has the freedom to choose to open, close or delete any social media account he or she owns.

Whilst an individual may "own" his or her online data, by virtue of signing up to a social network and agreeing to the terms of service on sign-up, he or she gives various permissions to use their online data for a variety of purposes (such as advertising).

Although there is often an express limit on the use of the online data within a network's terms of service, the question of whether the individual gives implied consent on sign-up is a contentious issue.

Do social media companies need to inform individuals that they are sharing their data?

Most social media companies share user data with third party companies and will often operate partner programmes for this very purpose. Until GDPR comes into effect in May 2018, it is enough for social media companies simply to state how they will share individuals' data (usually within a privacy notice, policy or terms of service agreement). However, under GDPR, consent to process and use an individual's data can no longer be implied. As such, consent merely by agreeing to an operator's terms of service on sign-up will no longer be enough. Companies will not be permitted to bundle GDPR-standard consents with provisions dealing with other matters. They will have to put in place measures enabling consent to be withdrawn as easily as it is given. Consent must be unambiguous to be effective.

Many companies seek to position their data processing activity as being in their "legitimate business interests". In the social media context, it may well be the case that sharing data is in an organisation's legitimate interests (for example, to enhance the quality of service provided to a user). However, companies taking this approach have to weigh up their business interests against the risks to individuals' privacy rights. In order to minimise their exposure to costly litigation and enforcement action, they must be able to show that careful consideration has been given to these competing factors and that the assessment of them has been appropriately documented.

In any event, GDPR requires the business to ensure that individuals are informed about data sharing practices before their information is shared. Based on the litigation and regulatory investigations already commenced for alleged misuse of data, the potential costs can be very

The EU General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) was passed in 2016 and will become law on 25 May 2018. As a Regulation, it is directly applicable in all EU member states and does not need to be transposed into national law. It does not have retrospective effect, so will not apply to the alleged conduct in this case, but it makes important changes to existing laws, which will substantially increase businesses' obligations and potential exposure in the event of breaches.

Key changes include:

- Substantially increased sanctions
- Greater harmonisation of rules across the European Economic Area (EEA)
- Extension of the regime to regulate processors as well as controllers
- A series of changes building on the existing data protection principles, making them stricter in various respects and introducing new compliance burdens
- New accountability and breach reporting requirements

Territorial scope

GDPR significantly expands the territorial reach of EU data protection and privacy rules. This means that many organisations, including social media companies (and any others which acquire or use individuals' online data) based entirely outside of the EU, will find themselves caught by GDPR. The regulation applies to non-EU companies if the data processing is carried out in order to offer goods or services to, or to monitor the behaviour of, individuals within the EU.

Penalties

Failure to comply with the requirements of GDPR exposes a company to unprecedented regulatory risk. Fines reach levels commensurate those imposed for anti-trust violations for the most serious breaches (up to EUR 20 million or four per cent of global turnover - whichever is higher).

significant, even where the allegations remain to be proven. Recent events are likely to prompt social media companies to include even more prominent privacy reminders and expand online privacy notices.

What are individuals' rights in respect of their online data?

GDPR strengthens individuals' rights over their "personal data" (which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier - such as name, identification number, location data or any online identifier). In particular, individuals can require those holding their personal data to:

- delete the data where there is no compelling reason for continued processing - this "right to be forgotten" has previously been recognised by the EU Courts but is now codified. It extends to a third party handling data on their behalf and requires them to erase links to, and copies or replications of, the personal data in question.
- provide individuals with a copy of the information an organisation holds about them, the reasons why this information is being processed, details of whether the information will be given to any other organisations or persons and, where available, the source of the data - the time limits for doing so have been shortened and fees abolished.
- transfer their personal data back to them in a downloadable, structured and machine-readable format.

There is no equivalent to GDPR in the US and no comprehensive set of privacy protections for the collection, storage and use of personal information. Instead, these requirements are imposed through contractual documents such as terms of service and privacy policies. There are some relevant protections in state law and some additional requirements imposed in certain industries such as financial services and healthcare, although none are as comprehensive as GDPR. The absence of a defined legal framework in the US on these issues increases the level of risk for the business community given the availability of numerous civil remedies (for example, breach of contract, negligence and fraud) and the readiness of US claimants to pursue them; and is compounded by the extensive extraterritorial reach of GDPR.

Recent events are likely to move large numbers of individuals concerned to exercise their rights, whether to prevent future misuse or to explore whether they may have claims against social media companies or other businesses involved in the processing of personal data. The volume and complexity of complaints may present significant practical issues. Now that these issues are firmly in the public domain, the press, politicians and enforcement agencies in various jurisdictions are likely closely to scrutinise the speed and completeness of companies' responses. Delays or any perceived lack of transparency are likely to generate negative publicity and may lead to separate, more forceful, action by investigating authorities and by the courts.

What are the legal limits on how third parties may use individuals' data?

Much depends upon documents such as the terms of service and privacy policies to which social media users sign up. For example, Facebook's publicly available data privacy policy appears to permit Facebook to share certain non-personally identifiable information (meaning data that does not include an email address or financial information) with third party advertising analytics vendors and technical infrastructure providers subject to strict confidentiality obligations.

However, there are some legal restrictions, which are set to be expanded under GDPR. Existing EU data protection rules set out the conditions by which personal data should be processed. These rules also impose additional controls on the processing of 'sensitive personal data'. This includes data concerning, for example, racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, health or sex life. Processing of this type of sensitive data requires explicit consent in addition to meeting the conditions for processing.

GDPR will also enhance current rules on profiling and the use of automated decision-making techniques to make decisions which have a legal effect on individuals or otherwise significantly affect them. For social media companies, this will represent a significant shift from what used to be considered industry practice.

Where and how might claims be pursued in respect of the misuse of data?

On both sides of the Atlantic, claimant lawyers are gearing up for action. Information provided to social media companies rapidly crosses national borders, giving potential claimants considerable flexibility to choose where to pursue claims. Various procedural mechanisms enabling claimants to join forces, the ready availability of litigation funding and a comparatively claimant-friendly disclosure regime could make the English Courts an attractive forum. Claimants may also seek to take advantage of particular features of other legal systems, such as that of the Netherlands, where there are established mechanisms allowing consumer organisations and other interest groups to claim declaratory or injunctive relief on behalf of injured parties and its "opt-out" certification of damages in class settlements.

In broadly analogous decisions decided to date, English judges have shown some willingness to provide data subjects affected by the misuse of private information with a remedy, through claims for misuse of private information, breach of confidence and/or breaches of EU data protection legislation. In particular, they have recognised that "damage" in the relevant EU directive includes non-pecuniary damage for distressing invasions of privacy, and that compensation would be recoverable for any damage suffered following a data breach. There has not though yet been a major decided case clarifying their approach to how such damages should be calculated.

In future litigation, we expect a particular focus on any investigation reports or preliminary findings as to the cause of a data breach, given that they are likely to be fertile material for claimants seeking to bolster their claims.

GDPR expressly contemplates civil litigation against data controllers and processers. It provides for compensation for data subjects who have suffered "material or non-material damage" as a result of a breach. It also contemplates consumer protection bodies bringing claims on subjects' behalf. This increases the prospect of a proliferation of civil litigation on these matters.

In the US, investors and users have already filed class actions based variously on allegations that Facebook breached its own data privacy policies and California's Unfair Competition Law by making materially false and misleading statements. Other users may attempt to bring a breach of contract claim for violations of Terms of Service and Privacy Policies. The prospects of such claims succeeding will be highly fact sensitive but claimants are likely to encounter some difficulties in establishing that they have suffered an economic loss as the result of the use of their data. Nevertheless, the risk that such litigation creates for those alleged to have misused personal date is acute.

Which investigating authorities should businesses be concerned about?

To date, the allegations against CA and Facebook have sparked investigations by the UK Information Commissioner's Office (ICO) and the US Federal Trade Commission (FTC). Both the ICO and the FTC are enforcement authorities whose remits include investigating and taking action in respect of breaches, data protection, and privacy. In the US, numerous state Attorneys General may open separate investigations. In addition, the UK Electoral Commission has commenced an investigation looking into possible data misuse in connection with the 2016 Brexit referendum.

The ICO has a relatively narrow remit to investigate and take action in respect of breaches of data protection and privacy legislation. Its investigative and

enforcement powers, resources and ability to impose penalties have historically been quite limited compared to other enforcement agencies. Fines imposed have not been of the same order of magnitude as those imposed on businesses for other types of misconduct. However, its powers, and its confidence in using them, are expanding and it is notable that the ICO has shown a willingness to use its criminal investigation powers to secure access to material (and has adopted a high profile approach when doing so).

The FTC has sought to hold companies accountable for breached cyber defences and other violations based on its general authority to monitor "unfair or deceptive acts or practices in or affecting commerce" under Section 5 of the FTC Act. FTC claims are generally premised on misleading advertising or disclosure. Facebook and the FTC entered into a settlement in 2011 which required Facebook to obtain consent prior to sharing consumer information beyond the scope permitted by a user's privacy settings. If the FTC determines that the settlement was violated, Facebook could be liable for as much as $40,000 per violation, which could lead to a significant penalty if 87 million users were affected.

In the US, states have been at the forefront of privacy and consumer protection and have been aggressive in the enforcement area. State Attorneys General can pursue an enforcement action if they determine there are violations of the rights of consumers in their state. Already, Attorneys General in Connecticut, Massachusetts, New York, Oregon, and Pennsylvania have made public statements regarding Facebook's conduct and may open investigations.

In addition to enforcement action, US and UK legislators are taking a keen interest in the allegations and have already summoned senior Facebook and CA executives to appear before them. UK Parliamentary Select Committees and their US Congressional counterparts have wide ranging powers to investigate. Proceedings before such bodies often involve organisations and senior individuals within them being strongly criticised not only for breaches of law and regulatory requirements but also on the basis of highly subjective ethical judgements. As other businesses have found to their cost, injudicious testimony before these bodies can lead to substantial reputational damage.

At present, the focus of inquiries is on social media companies and political consultants. However, data are also harvested, exchanged, sold and purchased in all manner of commercial contexts. As a consequence of the current allegations against CA and Facebook, other regulators and enforcement authorities will develop an interest in the way in which data is obtained and used by organisations in the areas for which they are responsible and more generally. Politicians will turn their attention to the extent to which data sharing (and potentially misuse) pervades the business operations of other types of organisations. Examples of scenarios where organisations' conduct may come under scrutiny include the use of data obtained by banks and insurance companies in the course of transactions carried out for or with individuals and the sharing and use of information about customers and their habits and preferences obtained by retailers through loyalty programmes.

How should businesses react to allegations of suspected data misuse?

Many more details will emerge from the investigations concerning Facebook, CA and whichever organisations are the next targets of public, political and regulatory scrutiny. For now, it is telling that a major focus of the reputational (and therefore the very real financial) impact upon Facebook has been what it knew about the way in which individuals' data were being used, and when. There will be continued focus on whether Facebook adequately investigated the position or whether it denied the allegations for too long.

In the interests of getting to the bottom of the facts and responding to law enforcement agencies, governments, stakeholders and the public, it is tempting for businesses to rush into commencing an internal investigation. However, before doing so, it is critical to give careful

consideration to the objectives and scope of any investigation.

A credible and thorough investigation can be an effective tool in reducing public backlash, investor withdrawal, regulatory/government scrutiny and potential censure, fine or conviction. However, an investigation can also create risks for the company which, with careful thought, can be mitigated (although probably not eliminated).

In some jurisdictions, facts uncovered by an internal investigation may not be protected by legal professional privilege, with the result that those facts may be disclosable to enforcement agencies and future civil litigants. They also run the risk of enforcement agencies alleging that the company has "trampled the crime scene" where, for example, data have been extracted in a non-forensic way or employees have been interviewed for their first accounts of what happened. In order to manage these risks and maximise the benefits of any investigation, scoping an investigation properly and early engagement with lawyers (and, in some cases, with law enforcement agencies) is essential.

Investigating agencies quickly get on top of the facts. They have access to large amounts of information, sometimes more information than the company under investigation itself. It is therefore essential to gain an early understanding of the expectations of each enforcement agency involved and the scope of their powers and propensity to cooperate with other agencies.

Conduct under investigation can generate significant parallel – or follow on – civil litigation. From a practical perspective, this can create challenges in terms of resources as companies can be fighting legal battles on several fronts at the same time. Where the litigation is occurring in parallel with any investigation, it can create tensions and risks that need to be carefully managed. It may be possible – although it can be difficult and not automatic – to obtain a stay of the civil proceedings whilst any criminal investigation takes its course. A company under investigation which anticipates follow-on litigation will also have to make decisions about the scope of any investigation since, as noted above, in certain jurisdictions the product of the investigation may not be protected by legal professional privilege.

Investigations, whether they are carried out by organisations themselves, their lawyers or enforcement agencies, are typically long and complex. Even where allegations have not yet been made or details of the matters being examined do not explode into the public domain at the outset, there is an ever present risk that they may do so. This necessitates careful contingency planning and an ability to respond nimbly and credibly to allegations. Commercial interests and reputations must be protected as far as possible whilst still demonstrating to investors, customers, staff and the wider world that matters are being taken seriously and legitimate concerns acted upon. As may turn out to be the case in this instance, what businesses do (or do not do) in the hours and days following allegations usually lives just as long in the memories of key stakeholders as the eventual outcome of investigations.

CONTACTS

London

Julian Acratopulo
Partner
Litigation and arbitration
T: +44 20 7006 8708
E: julian.acratopulo
@cliffordchance.com

Jonathan Kewley
Partner
Tech
T: +44 20 7006 3629
E: jonathan.kewley
@cliffordchance.com

Luke Tolaini
Partner
Enforcement and crisis management
T: +44 20 7006 4666
E: luke.tolaini
@cliffordchance.com

Mark Comber
Lawyer
Tech
T: +44 20 7006 2398
E: mark.comber
@cliffordchance.com

Jennifer Mbaluto
Senior Associate
Tech
T: +44 20 7006 2932
E: jennifer.mbaluto
@cliffordchance.com

Zoe Osborne
Director – Investigations
Enforcement and crisis management
T: +44 20 7006 8293
E: zoe.osborne
@cliffordchance.com

Kate Scott
Senior Associate
Litigation and arbitration
T: +44 20 7006 4442
E: kate.scott
@cliffordchance.com

Chris Stott
Senior PSL
Enforcement and crisis management
T: +44 20 7006 4231
E: chris.stott
@cliffordchance.com

New York

Herbert Swaniker
Lawyer
Tech
T: +44 20 7006 6215
E: herbert.swaniker
@cliffordchance.com

Midori Takenaka
Lawyer
Tech
T: +44 20 7006 1593
E: midori.takenaka
@cliffordchance.com

Samantha Ward
Senior Associate
Enforcement and crisis management
T: +44 20 7006 8546
E: samantha.ward
@cliffordchance.com

Robert Houck
Partner
Litigation and arbitration
T: +1 212 878 3224
E: robert.houck
@cliffordchance.com

New York

Celeste Koeleveld
Partner
Enforcement and crisis management
T: +1 212 878 3051
E: celeste.koeleveld
@cliffordchance.com

Daniel Silver
Partner
Enforcement and crisis management
T: +1 212 878 4919
E: daniel.silver
@cliffordchance.com

Benjamin Berringer
Associate
Litigation and arbitration
T: +1 212878 3372
E: benjamin.berringer
@cliffordchance.com

Daniel Podair
Associate
Enforcement and crisis management
T: +1 212 878 4989
E: dan.podair
@cliffordchance.com

Paris

Dessislava Savova
Partner
Tech
T: +33 14405 5483
E: dessislava.savova
@cliffordchance.com

Washington

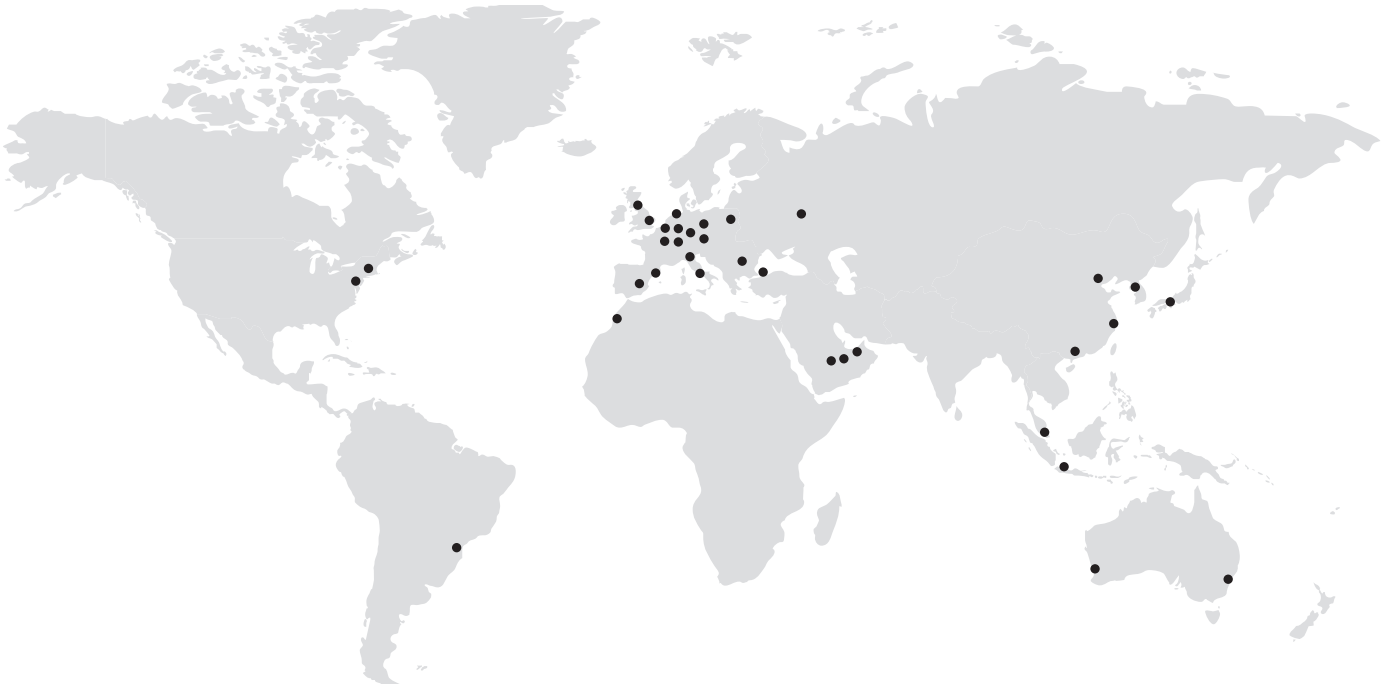
Megan Gordon
Partner
Enforcement and crisis management
T: +1 202 912 5021
E: megan.gordon
@cliffordchance.com

Steve Nickelsburg
Partner
Litigation and arbitration
T: +1 202 912 5108
E: steve.nickelsburg
@cliffordchance.com

David Rabinowitz
Associate
Enforcement and crisis management
T: +1 202 912 5436
E: david.rabinowitz
@cliffordchance.com

NOTES

OUR INTERNATIONAL NETWORK
32 OFFICES IN 21 COUNTRIES



Abu Dhabi
Amsterdam
Barcelona
Beijing
Brussels
Bucharest
Casablanca
Dubai
Düsseldorf
Frankfurt
Hong Kong
Istanbul
London
Luxembourg
Madrid
Milan
Moscow
Munich
Newcastle
New York
Paris
Perth
Prague
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.

Riyadh*

*Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

J20182703181416