ITN SOLICITORS

Media contact: Julia Pacetti, julia@jmpverdant.com, (917) 584-7846

London, May 5, 2018 — Yesterday, the U.K. **Information Commissioner's Office** (ICO) issued an Enforcement Notice to **Julian Wheatland** and **SCL Elections Limited**, the parent company of **Cambridge Analytica**, ordering the **SCL Group** to disclose the full voter profile of American **Professor David Carroll**, or potentially face a criminal penalty. The order is pursuant to Carrol's **Subject Access Request** (SAR) under the **U.K. Data Protection Act** (DPA). The Enforcement Notice advises Wheatland that in light of the seizure of equipment and information following a warrant executed at SCL's New Oxford Street offices, the ICO will prioritise recovery of relevant information if SCL provides relevant passwords.

Carroll made an SAR on January 10, 2017, and received a response from the SCL Group on March 27, 2017. In its Enforcement Notice, the ICO reports that SCL Elections asserted that Carroll was no more entitled to make an SAR under the DPA "...than a member of the Taliban sitting in a cave in the remotest corner of Afghanistan." The ICO has roundly rejected this argument that Carroll is not entitled to his data because of his American nationality.

Ravi Naik, the U.K. solicitor representing Carroll in the case, states,

"It is regrettable that it has taken litigation to get to this point but we are pleased to see the Information Commissioner agree with Professor Carroll's complaint. The Information Commissioner has also made the penalties for non-compliance very clear and we now expect full disclosure from SCL and its subsidiaries within 30 days. Professor Carroll has long fought for his data under the DPA, and he has now been vindicated". Naik continues, "We expect to receive disclosure from Cambridge Analytica on matters of global significance. The ICO's decision will provide us all with answers about what Cambridge Analytica did with people's data, how it was used and who it was given to. Professor Carroll has really taken a stand at his own personal risk and cost. We were always confident that he was in the right to request his data and are very pleased that the ICO has confirmed his position."

To view the enforcement notice on the ICO website, please visit this link:

https://icosearch.ico.org.uk/s/search.html?collection=ico-meta&profile=decisions&query

The Enforcement Notice finds that SCL has not cooperated with the Commissioner Elizabeth Denham's investigation of this matter, and that the company must be holding further heretofore undisclosed data regarding Carroll in order to have generated his profile and "model."

The notice compels SCL to provide Carroll with: (a) a description of the personal data processed by the data controller about him; (b) a description of the purposes for which that data are being processed; (c) a description of the recipients of his data; (d) copies of the information constituting his personal data in an intelligible form and in accordance with the requirements of section 7 of the DPA and the Sixth Data Protection Principle; and, (e) a description of the source of Carroll's personal data.

Carroll states, "Last summer, just in time for Independence Day, I filed a complaint with Cambridge Analytica's regulator in the United Kingdom, the Information Commissioner's Office. We've offered the registered data controller for Cambridge Analytica, SCL Elections Ltd, ample opportunities to respond to my valid concerns about where, how, and with whom they have processed and exploited my personal data. It has been increasingly distressing over the past year to witness their lack of interest in full cooperation, and to imagine why. I trust that the ICO's Enforcement Letter now impresses upon Mr. Wheatland the authorities vested in Commissioner Denham by the U.K. Data Protection Act, and her jurisdiction over my case."

About the Case

Following revelations of Cambridge Analytica's possible influence over the U.S. presidential election in 2016, American academic David Carroll, through his British solicitor Ravi Naik, has brought a landmark case to the British High Court that leverages the U.K. Data Privacy Act against Cambridge Analytica and their parent company SCL Group Ltd., demanding full disclosure of the private information the company holds on him. The claim is the first of its kind against Cambridge Analytica and has the potential to reveal critical details about the data that the company holds on millions of people worldwide, and whether collection and use of that data has broken U.K., U.S. or other laws. The claim demands disclosure of: (a) the personal data set on Carroll; (b) all sources from which they gathered this data; (c) the model that resulted from analysis of the data; and (d) the names of Cambridge Analytica's clients who have received or benefited from this information. Through this disclosure, the case has the potential to elucidate a clear

picture of Cambridge Analytica's activities surrounding the U.S. presidential election, to probe the boundaries of permissible use of personal political data, and to create a path to better protect sensitive, proprietary personal information in the future.

The Legal Basis for the Case: U.K. versus U.S. Jurisdiction

Many have asked why Carroll is trying his case in the U.K. as opposed to the U.S. While the election controversy surrounding Cambridge Analytica's data practices pertains to the U.S. population and government, Cambridge Analytica is only a shell company in the U.S., hence any legal claim against it in U.S. courts would likely be ineffective. Furthermore, while the U.S, does have a certain amount of data protection legislation in place, such measures are far less stringent than those of the U.K.

Cambridge Analytica and its parent company SCL are based in the U.K. and are thus subject to the U.K. Data Protection Act (DPA). Section 7 of the DPA, through use of a mechanism called a Subject Access Request (SAR), entitles any individual, regardless of nationality, to full disclosure of any personal data used by a company registered in the U.K. Based on the information known to date, the DPA is currently the only applicable law that can legally compel Cambridge Analytica, through the courts, to reveal all information pertaining to personal data records collected, manipulated and then sold by the company. Only once Professor Carroll gains full disclosure pursuant to his SAR request can we know if U.S. law was broken or not, and whether his rights — and those of millions of others — were violated.

About the Data Protection Act

The U.K's Data Protection Act (DPA), passed in 1998, controls how personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called "data protection principles." Stipulations for the use of personal data include: that it is used fairly and lawfully; used for limited, specifically stated purposes; used in a way that is adequate, relevant and not excessive; kept secure; and not transferred outside the European Economic Area without adequate protection. The DPA also provides special legal protection for sensitive subjects such as political opinions and religious beliefs.

Notable cases where the DPA has been invoked include claims of misuse of personal information brought against British tabloid newspaper the Mirror by Naomi Campbell, and Hello! magazine by Catherine Zeta-Jones and Michael Douglas. It was also cited, in part, during the News of the World "phone hacking" scandal and subsequent investigations, which led to the paper's closure in 2011.

The DPA affords individuals, irrespective of nationality, the right to view the data an organization holds on them by filing a Subject Access Request (SAR). David Carroll submitted an SAR to Cambridge Analytica in January 2017 and received a response on 27 March 2017. The results of the SAR confirmed that his U.S. voter information was processed in the U.K. When he submitted his SAR, Carroll did not anticipate uncovering information that has since become relevant to the various investigations underway in the United States relating to the 2016 presidential election.

Incomplete Subject Access Request Disclosure

While Cambridge Analytica's response to Carroll's SAR was troubling, containing sensitive and potentially illegal material such as voter registration data not readily available in the public domain, it fell significantly short of explaining how Cambridge Analytica were able to create a bespoke political profile or "model" with the limited variables they claimed to have used.

The personal data provided was insufficient to support Carroll's 'headline' personal profile, which appeared to be based on further information about him that was not provided in Cambridge Analytica's response.

The scant details provided also stand in direct contrast with Cambridge Analytica's own publicly confirmed claim by company Chief Executive Officer, Alexander Nix, stating that the company has "up to 5,000 data points on over 230 million American voters." This discrepancy has prompted Carroll to take legal action against Cambridge Analytica for failure to comply with section 7 of the U.K.'s Data Protection Act.

Incomplete Disclosure on Modeling

Cambridge Analytica employs "re-identification" techniques and technologies, whereby anonymous data and information are combined with other information to "re-identify" an individual from anonymous data. It is also often described as "de-anonymization" or "data-matching." Using re-attached data, Cambridge Analytica developed and then sold psychographic "models," or political profiles, of thousands of individuals. These models rank a person's political views, categorized into 10 variables, by order of perceived importance. Cambridge Analytica employed the models to micro-target U.S. voters, individually and in groups, by their personality types and susceptibilities to personalised messages based on their personal data and online behaviour.

An example of this practice would be the "reattachment" of an individual's consumer data with their voter data and political behavior. In Professor Carroll's view, this technique does not comply with people's expectations of privacy policies, which seek to assure that

behavioural data can be safely shared with third-parties once personal identifiers are removed. Thus, it is important that lawmakers, academic researchers and journalists have the ability to investigate whether or not re-identification, or data-matching, is occurring within the information industry to better understand the data supply chain and the question of whether laws or civil liberties are being violated. This is especially true for voter analytics, where a voter's consumer behaviour may be re-attached to their voter registration information. In some U.S. states, the monetization of voter data is illegal, and manipulation of voter data by non-U.S. citizens is a federal crime.

Incomplete Disclosure of Beneficiaries

According to the Information Commissioner's Office, the U.K. government body that oversees the enforcement of the DPA, an individual who makes an SAR, in addition to receiving the data itself, should be told the reasons their data is being processed and whether it will be passed on to other organisations. While the response to Carroll's SAR provided a summary of the types of clients that they might share his data with, such as "political campaigns" and "commercial entities," it failed to indicate the actual organisations with which the data had actually been shared, again falling foul of section 7 of the DPA.

Incomplete Disclosure of Sources of Data

Cambridge Analytica also did not provide the requisite information regarding the source, or sources, of the personal data, again in violation of section 7 of the DPA. The SAR response only stated that they had obtained it from "reputable data vendors" and "research partners."

Based on basic modeling principles, it is clear to experts that the data sources disclosed do not support the models created. Full transparency on the sources of the data used is necessary to understand how each individual's online or other behaviour has led to the generation of personal profiles. It will also uncover the breadth of information needed to make sophisticated predictions about political beliefs – a revelation that will be of widespread interest, and which could have massive ramifications for the issues of data privacy, micro-targeted marketing and political campaigning in years to come.