WITNESS STATEMENT

HOUSE COMMITTEE ON JUDICIARY

OREGON STATE LEGISLATURE

BILL HB 2866

Relating to required actions with respect to personal information of resident individuals.

MARCH 12, 2019

DAVID R. CARROLL

ASSOCIATE PROFESSOR OF MEDIA DESIGN

PARSONS SCHOOL OF DESIGN

THE NEW SCHOOL

NEW YORK

Dear Chair Williamson, Vice Chairs Gorsek and Sprenger, and the Committee,

I write to the committee today for this hearing as an individual and advisor to the Digital Privacy Alliance. Through my academic research and industry experience I have become known for challenging Cambridge Analytica and related companies in the United Kingdom under the Data Protection Act of 1998 and through criminal enforcement actions of the Information Commissioner's Office. I am pleased to address the committee, having been afforded similar opportunities to give evidence about my Cambridge Analytica data quest to state legislature committees in Illinois, Nevada, and my home state of New York. I have also given confidential evidence to the Senate Select Intelligence Committee (SSCI), House Permanent Select Intelligence Committee (HSPCI), Senate Judiciary Committee, and House Judiciary Committee. Internationally, I have given public evidence to the UK Parliament Select Committee on Digital, Culture, Media, and Sport (DCMS), Canada House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), and the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE). I have tried to publicize my personal story to bring attention to the wider public interest issues in the press. I've been featured in an upcoming Netflix documentary released later this year that will make complex issues more easily understandable to general audiences. The public awareness of data rights issues in the aftermath of the Cambridge Analytica controversy will continue to reverberate through multiple democracies around the world. Last week, on March 4, when the House Judiciary Committee released its document request list, Cambridge Analytica and SCL Group Ltd. were listed, as well as two directors, Alexander Nix and Julian David Wheatland, and former employee and known subject of the Special Counsel's investigation, Brittany Kaiser.

The Cambridge Analytica controversy is crucially relevant to the consideration of HB 2866, which as proposed, grants residents of Oregon certain Rights of Access and Consent with regards to their location and audiovisual personal data. This would help align the state with the prevailing trend of affording data subjects the right of access (the right to know, the right of disclosures) and the right to revoke consent. These are fundamental human rights under the EU charter. Despite the privacy protections implicit in the Constitution, the United States is now decades behind our closest allies across the Atlantic when it comes to citizens demanding adequate data protection law and enforcement.

In a remarkable twist of history, I discovered that US voter data was processed in the UK during the 2016 campaign and earlier by companies related to Cambridge Analytica, namely SCL Elections Ltd. We could prove this because the UK Data Protection Act of 1998 required SCL to register as a data controller with the Information Commissioner's Office, the independent regulator of the DPA. As a function of being the registered data controller on behalf of Cambridge Analytica, and under Section 7 of the UK DPA of 1998, it was obliged to respond to my Subject Access Request in January of 2017. The cover letter and Excel spreadsheet provided to me by SCL Group Ltd. in March 2017 can be provided to the committee if desired.

Geolocation information was provided as a data point field in the Cambridge Analytica Subject Access Requests of other US citizens that I have seen, although my file does not contain a latitude and longitude field. This may serve as an example of how the right of access empowers citizens the ability to compare their voter files. How else could we begin to understand how we are selected by campaigns on the important topics that animate our democracy. We know that Cambridge Analytica may have used geolocation data harvested from Instagram and combined it with voter files because, Professor Jonathan Albright from Columbia Tow Center has published an analysis of source code publicly available. The source code was removed shortly after Professor Albright brought attention to it.[1]

It is reassuring to see the language "deriving inferences from" as this is precisely the subtle but crucial bright line to draw as a new fundamental civil right that the states must urgently assert, reinforcing this notion in the California Consumer Privacy Act (CCPA), in advance of rapid developments in machine learning, algorithmic accountability, and artificial intelligence. In the UK Information Commissioner's report on the Cambridge Analytica scandal, an unambiguous recommendation is made to further regulate inferred data as personal data.[2]

[1] https://medium.com/tow-center/cambridge-analytica-the-geotargeting-and-emotional-data-mining-scripts-bcc3c428d77f

[2] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/

After seizing the servers belonging to Cambridge Analytica/SCL Group Inc under criminal warrant about a year ago now, the ICO has undertaken the most complex data forensics investigation in history. The ICO has also prosecuted SCL Elections Ltd for ignoring their Enforcement Order to fully disclose my personal data and fully address the disclosure requirements mandated under section 7 of the UK DPA of 1998. SCL Elections pled guilty on January 9, 2019 and paid a fine of £15,000 but I have yet to recover full disclosure of my Cambridge Analytica voter profile.[3]

The Cambridge Analytica story offers legislatures a perfect worst-case scenario to illustrate the fundamental necessity to catch up with peer nations and enshrine data protection rights to our citizens. We can understand more easily how data protection, privacy rights, and their enforcement is more inextricably linked to free and fair elections than ever before in history. It shows lawmakers why the right of access, the right to know, is the underlying bedrock right that all other data protection and data privacy rights must be built upon. All 50 states need to ratify the right of access at the minimum, to even begin to address the problem of data abuse and privacy invasion in the 21st century.

The Cambridge Analytica scandal also teaches the public and the members at statehouses how data modeling creates inferences about our beliefs and leads to predictions about our future behaviors and attaches them to our personal information and identities. They do this without our knowledge or consent and make it essentially impossible to opt-out, even when we chase our personal data into other another nation's jurisdictions where we discover that we have standing to exercise more rights than our own country affords us. We can even trigger enforcement action in countries with data protection rights if we can prove we are data subjects through the right of access. In fact, the only criminal prosecution of Cambridge Analytica/SCL in the world, to date.

Data models can also be detached from our personal data as a means to shield them from disclosure and revocable consent. We were able to learn from a BBC program (never broadcast in the US) titled *Secrets of Silicon Valley* that Alexander Nix, former CEO, acknowledged that "legacy data models" from the Ted Cruz campaign carried over into the Donald Trump campaign.[4] It's up to the states to help recapture control of voter files now that we know that foreign companies run by executives are willing to mislead lawmakers in the US and UK.

Next week I will travel to London to witness my trial challenging the administrators funded by the parent company of Cambridge Analytica, Emerdata Limited a British holding company in turn mostly owned by Cambridge Analytica Holdings LLC. We have concerns that the administrators are not respecting the data protection rights of US voters that have been

[3] https://www.theguardian.com/uk-news/2019/jan/09/cambridge-analytica-owner-scl-elections-fined-ignoring-data-request

[4] https://twitter.com/profcarroll/status/976095078673510400

recognized and enforced by the Information Commissioner's Office. The trial introduces the notion of a data creditor and teaches us that data privacy law ultimately intersects with bankruptcy law. What happens when a rogue actor gets caught and goes out of business? Do citizens and consumers lose their rights in that event?

The complexity of issues that collide around the question of data privacy are immense but the language being proposed for HB2866 offer simple and clear guardrails around fundamental rights, the need to contend with data models and inferences, and the need to expand the categories of data to include geolocation and audiovisual identity information as machine learning develops various types of fingerprinting technologies. Oregon has an opportunity to lead the nation in enshrining the new data rights of the 21st century. Key questions of democracy are at stake. Let Cambridge Analytica serve as a litmus test for legislators to evaluate badly needed protections.

Please do not hesitate to follow up with me if I can be of further assistance in the cause to better protect the data rights of the residents of Oregon.

Yours faithfully,

David R. Carroll
Associate Professor
The New School