ORAL TESTIMONY PRESENTED TO
NEW YORK STATE SENATE STANDING COMMITTEE ON
CONSUMER PROTECTION AND INTERNET & TECHNOLOGY

NOVEMBER 22, 2019, 11 AM
250 BROADWAY, SENATE HEARING ROOM, 19TH FLOOR
NEW YORK, NY 10007

BY DAVID CARROLL
ASSOCIATE PROFESSOR OF MEDIA DESIGN
PARSONS SCHOOL OF DESIGN, THE NEW SCHOOL
NEW YORK, NY 10011

Chairs Thomas and Savino, and the members of the committee on Consumer Protection and Internet & Technology, I thank you for the opportunity to give evidence to you today. I hope to contribute towards your work developing the necessary legislation to grant New York residents basic data rights as you take up the essential effort to safeguard personal information from mass data abuse, a condition that we cannot simply accept as the cost of doing business in the information age. We're in a rare, fleeting moment when broad support for new privacy regulation is booming as trust in tech platforms has broadly deflated.

I appear here today because I have become known for mounting a significant effort to repatriate my personal data from Cambridge Analytica, the notorious company synonymous with "doing bad things with people's data in elections" and causing a data privacy awakening around the world, especially in the United States. We should not even need to repatriate our voter profiles, but strangely, our voter files were exported to the UK in connection with the US elections. Simply by filing a Subject Access Request, we quickly proved that the UK Data Protection Act of 1998 would apply in the case of Cambridge Analytica because it was a UK entity, registered with the UK Information Commissioner's Office as a data controller.

We unlocked a fundamental purpose of the right of access, the right to know, as a new important safeguard for elections and the democratic process. We did not pursue this effort as purely partisan posturing. Originally, the effort to recover my data derived from academic curiosity to test if this legal condition would even apply to Cambridge Analytica. It turns out it did, and the UK has jurisdiction over Cambridge Analytica's servers, which were seized under criminal warrant, and whose forensic report is due by the British data cops very soon. My effort of course became personal, and unavoidably political, when my own voter data and the legally mandated disclosure of it eventually became a criminal matter in the UK courts and noted by Parliament select committees. I appreciate being recognized by New York State, today, in the context of this hearing on protecting New Yorker's data online. I'm glad I can finally help bring this conversation home.

The recognition of how a UK company broke UK law in the US elections is not well known nor well understood here in America. Perhaps the original Netflix documentary, *The Great Hack*, which includes aspects of my quest to seek the truth from Cambridge Analytica in England offers Americans the clearest glimpse yet into the shadowy world of defense contractors building up new business development opportunities in the elections management and voter analytics industry as the free flow of personal data in unregulated markets affords the types of mass data abuses that Cambridge Analytica will forever symbolize.

For me, it has been a learning process, appreciating the vision of the EU Charter, which enshrined data protection as a human right along with freedom of expression and freedom to marry, and so on. The architects of the modern creation of the EU were visionary in knowing that we would need fundamental data rights decades before the internet reshaped the world in unpredictable and unimaginable ways, posing new and unforeseen challenges to free and fair elections. Yet we hear a common critique that laws are always struggling to keep up with the latest technology while inhibiting innovation in the process. This concern is understandable, but there is still plenty of room to appreciate why we need data rights regardless. Our laws need our own future-minded upgrades to contend with the tomorrow of artificial intelligence. This is especially true now that we begin to grasp how our personal data is potentially being abused at scale by bad actors around the world and in connection with our elections.

This is why I'm here today emphatically showing my support for S.5642 THE NY PRIVACY ACT which seems to take some of its inspiration from the EU's GDPR while 'Americanizing' key concepts. It takes California's CCPA even further. As Microsoft announced that it will voluntarily grant US residents outside of California their CCPA data rights, it signals to us how the tech industry will embrace these new guardrails even beyond their territorial jurisdictions, especially as leaders step up and realize why building up a robust data protection regime in the United States is essential work of the 21st century.

There's a realization that in the twilight of the second decade of this millennium, we are at least 20 years behind Europe in constructing what's needed for enforceable data protection rights in the USA so that privacy is even a possibility. The State of New York plays a critical role in advancing the cause of data rights in America. Being an economic powerhouse like California, the successful passage of the NY PRIVACY ACT will help trigger a tipping point leveraging the ability of statehouses to iterate and refine legislation with greater agility than Capitol Hill. Americans are not waiting for Congress to get around to passing a GDPR for the USA.

As for the CCPA and the GDPR, many companies are well on their way to achieving compliance and adopting new data rights management tools already appearing in the marketplace in response to these new regulations. Whitespace in the zone of data privacy management entrepreneurship is opening up because new innovation and competition is yearning to breathe free in an otherwise stifled, consolidated, and disintermediated digital data-for-attention market. We want New York to be a leader in a new wave of privacy-by-design innovation as industry continues to adapt to Europe, California, and with your support, New York.

In particular, S.5642 offers crucial protections that build upon and extend aspects of the CCPA and GDPR, especially Section 10(xii) relating to inferred data described as personal data and restrictions on how profiles may be used adversely against the interests of data subjects. The bedrock of keeping data controllers accountable is the enforcement of access rights, the right to know about not just your personal information but also inferences made about you from models that process your data blended from an otherwise unknowable set of sources. The NY Privacy

Act affords strong but reasonable guidelines and mechanisms for data subjects to understand their rights and how to exercise them, which should include clear, de-obfuscated access to data inferred about us with concise explanations to achieve a fair legibility into concerns related to decision making and microtargeting.

As a New York resident myself, someone who has taken a significant private action against a registered data controller, SCL Elections Ltd. (aka Cambridge Analytica), in a data protecting state, such as the United Kingdom, I can appreciate why the NY Privacy Act preserves the right to endeavor to such private actions when data abuse is credibly suspected. My experience in the UK taking on a data rights legal challenge taught me how concerned citizens as data subjects can participate in turning the wheels of justice by establishing legal conditions for regulators to enforce data protection requirements on data controllers and prosecute their failure to comply with enforcement orders as necessary. Voting citizens must be granted legal tools to recapture certain kinds of controls to exert more autonomy over their personal data. Although there are many threats to consider, the problem of election integrity alone is one worth protecting with new transparency tools.

As for further suggestions to continue to amend and develop the NY Privacy Act, I think it is important for the co-sponsors, committee, and Senate more broadly to understand some of the particulars to how the Cambridge Analytica story really ended. The UK insolvency case ultimately nixed a US citizen's established subject access rights. Cambridge Analytica was able to achieve a moratorium shielding them from outstanding claims and so I never had my day in court over their very serious breaches of principal one of the UK Data Protection Act and the unfair creation of political profiles without rights or consent in connection with the US presidential elections in 2016, as declared and reported by the Information Commissioners.

Subsequently, Cambridge Analytica LLC was abandoned in New York Bankruptcy court making it difficult for the Federal Trade Commission to issue legal challenges against the defunct US entity for deceptive practices. No New York resident claimed ownership of the entity which of course operated offices in the state of New York, allegedly processing the data of all registered voters, and not just New Yorkers who had their Facebook data illicitly harvested. But thanks to

the Information Commissioner's seizure of the servers, there's still a chance my data can be recovered.

Perhaps the NY Privacy Act and/or the Bankruptcy code may need further amending to consider how data rights should persist when a data controller becomes insolvent and files for bankruptcy. Shouldn't data subjects continue to be able to exercise their subject access rights as a kind of data creditor before bankruptcy court given that their personal data consists of something of value to the entities and their creditors as a going concern? If we do not address the "bankruptcy loophole" of data rights, then we may not address a key lesson learned from the Cambridge Analytica scandal. An anonymous LLC company can become a registered data controller, acquire and recombine vast amounts of personal data, enriching public data, and generating inferences with potential adverse intents. Should a data subject attempt to fulfill a subject access request and the result of that request is legitimately challenged as to its adequacy, the data controller can simply file for bankruptcy and shed its potential liability for mass data abuse. Unless, that is, a data subject could become a data creditor when a company goes into bankruptcy, administration, or liquidation. Especially because the last gasp of Cambridge Analytica LLC and its scandalous lifetime occurred in New York bankruptcy court, and partially as the result of a New York voter pursuing private action abroad that helped expose mass data abuse liability in the process, it shows how the Statehouse might consider how consumer protection of data rights persists well into the endgame of a suspected or proven data abuser.

Whether or not New York's Privacy Act will prevent another Cambridge Analytica is an important litmus test especially because it was essentially a New York entity, allegedly owned by New Yorkers, which according to UK law, abused the data of New Yorkers in connection with elections in our state. There's clear need for Albany to act and protect New Yorkers from further abuse and harm now that we know how Cambridge Analytica was merely a canary in the coal mine of a dark and murky world where public data gets mixed with other data, including commercial data, and used in troubling ways within the democratic process. Until every New Yorker can exercise their data rights with confidence, we will not have the basic tools to root out and deter bad actors in the data economy, let alone help protect elections from abuse and interference.