

Court File No. 211/19

**ONTARIO
SUPERIOR COURT OF JUSTICE
(DIVISIONAL COURT)**

BETWEEN:

CORPORATION OF THE CANADIAN CIVIL LIBERTIES ASSOCIATION
and LESTER BROWN

Applicants

and

TORONTO WATERFRONT REVITALIZATION CORPORATION, CITY OF
TORONTO, HER MAJESTY IN RIGHT OF ONTARIO as represented by the
MINISTER OF INFRASTRUCTURE, HER MAJESTY IN RIGHT OF
CANADA as represented by the MINISTER OF COMMUNITIES AND
INFRASTRUCTURE, AND THE ATTORNEY GENERAL OF CANADA

Respondents

APPLICATION under sections 2 and 6(1) and 6(2) of the *Judicial Review Procedure Act*, R.S.O. 1990, c. J.1, as amended, and sections 2, 7, 8 and 24 of the *Charter of Rights and Freedoms*.

AFFIDAVIT

I, Ben Green, of New York City, in the State of New York, in the United States of America,

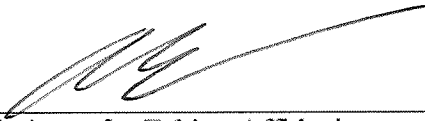
MAKE OATH AND SAY:

1. I am a PhD Candidate in Applied Math at the Harvard School of Engineering and Applied Sciences and an Affiliate at the Berkman Klein Center for Internet and Society at Harvard. I study the implementation and impacts of data science in local governments, with a focus on "smart cities" and the criminal justice system.
2. Attached here as **Exhibit "1"** is a copy of the report I have prepared in response to a request to give opinion evidence in this proceeding.

1
BG

3. Attached to my report is the Acknowledgement of Expert's Duty that I have signed as well as my curriculum vitae outlining my education, experience and credentials.
4. The attached report accurately describes the instructions I received, the issues I was asked to address, my opinion respecting each issue and the reasons for my opinion. I have also described the factual assumptions on which my opinion is based, my research, and the documents I relied on in forming this opinion.
5. I believe that my report is accurate, based on the available information. I have prepared this report to the best of my ability.

SWORN BEFORE ME by video conference from New York City, in the State of New York, to the City of Toronto, in the Province of Ontario, on April 29th, 2020.


 Commissioner for Taking Affidavits
(or as may be)

ALEXANDER EVANGELISTA / LSO# 76985D


 Ben Green

This is Exhibit "1" referred to in the Affidavit of Ben Green sworn
April ^{24th}....., 2020.



Commissioner for Taking Affidavits (or as may be)

ALEXANDER EVANGELISTA

BG

A. Qualifications

I am a scholar of municipal technology. I am a PhD Candidate at Harvard's School of Engineering and Applied Sciences (graduating in fall 2020), an Affiliate at the Berkman Klein Center for Internet and Society at Harvard, and a Research Fellow at the AI Now Institute at NYU.¹ My research focuses on the governance and social impacts of new technologies used by city governments. This research is informed by academic training as a data scientist, time spent working for the City of Boston as a data scientist, and collaborations with city data officers (in Boston, Seattle, San Francisco, and other cities) to develop effective and responsible privacy policies. My relevant publications include *The Smart Enough City*² (a book that analyzes and reviews the opportunities and dangers of smart cities) and "Open Data Privacy"³ (a report designed for municipal officials, about the privacy risks of data collection and use and about strategies for mitigating these dangers). I have a Master's degree in Applied Mathematics from Harvard University and a Bachelor's degree in Mathematics & Physics from Yale College.

B. Scope of Work

I am filing this report as a supplement to my first report, dated May 10, 2019. My comments in this report reflect my review of the affidavit of Kristina Verner sworn on January 17, 2020, new documents released by Waterfront Toronto and Sidewalk Labs, and new research and articles that have been released since my first report. In particular, I have reviewed the following new documents pertaining to the Quayside project:

- Master Innovation & Development Plan (MIDP)
- Master Innovation & Development Plan Digital Innovation Appendix
- Plan Development Agreement Threshold Issues
- Waterfront Toronto Draft Digital Principles
- Waterfront Toronto's MIDP Evaluation Consultation Discussion Guide
- DSAP Preliminary Commentary and Questions on Sidewalk Labs' Draft Master Innovation and Development Plan (MIDP)
- DSAP Supplemental Report on the Sidewalk Labs Digital Innovation Appendix (DIA)
- Quayside Evaluation Committee Report

Based on my review of these documents, my opinions regarding the broad privacy risks of the Quayside project remain the same as in my first report.

C. Executive Summary

Despite the statement made by Kristina Verner in her January 17, 2020 affidavit that the MIDP is still "evolving" and so therefore should not be subject to litigation,⁴ there is a vast weight of evidence regarding the harms of the data collection proposed in the Quayside project (and the likelihood of those harms arising). A great deal of scholarship and journalism have demonstrated

¹ I write only in my individual capacity, not on behalf of these organizations.

² Ben Green, *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future* (MIT Press, 2019).

³ Ben Green et al., "Open Data Privacy: A risk-benefit, process-oriented approach to sharing and protecting municipal data," *Berkman Klein Center Research Publication* (2017), <http://nrs.harvard.edu/urn-3:HUL.InstRepos:30340010>

⁴ Kristina Lynna Verner, *Affidavit* (2020), par 6.

the close link between smart city style widespread data collection and privacy harms.⁵ I find the Quayside project to be insufficiently attentive to these risks, in particular to rely on a definition of de-identification that goes against more than a decade of legal and technical scholarship regarding data privacy. Given the known risks of widespread data collection and the lack of clear and appropriate safeguards, I believe that the Quayside project will introduce severe privacy risks with very likely privacy harms resulting. If such concerns related to privacy are allowed to bear weight only after the plans are finalized, then more often than not it is too late for those concerns to be meaningfully addressed.

D. Analysis

The Notice of Motion served by Waterfront Toronto on January 17, 2020 states that “[t]he relief sought in the Amended Notice of Application is premature.”⁶ Reasons stated include that “[a]ny harms that may arise from this Project, including any potential *Charter* breaches are speculative at this time”⁷ (specifically noting that “[t]he privacy harms are also speculative”⁸) and that “[t]he remedial action sought by the applicants is not justified as the link between the action and the future harm is not capable of proof at this time.”⁹

This position reflects a lack of attention to the multiplicity of risks intertwined with the pervasive data collection that the Quayside project requires: this data can be used to re-identify individuals and learn sensitive information about people’s behavior, draw inferences about people’s behavior which can be used to manipulate and abuse individuals, and conduct widespread surveillance; it can also be released to a wide range of actors through data breaches. Describing these risks as merely “speculative” is contradicted by significant research and examples of the very real nature of these risks, and the harms that result when these risks come to fruition (which they frequently do). There is a great deal of literature demonstrating the close link between these forms of pervasive data collection and the resulting privacy harms.¹⁰ The most effective way to prevent these risks is not to view them as “speculative,” but to view them as inherently intertwined with data collection—and to work to counteract those risks with their pressing reality front of mind.¹¹

As security expert Bruce Schneier puts it, ‘data is a toxic asset and saving it is dangerous.’¹² Once data is collected, it is prone to be released. Moreover, once data is collected, it is prone to be used in unexpected, unintended, and often harmful ways. These harms are not merely “speculative,” as Waterfront Toronto claims, but have been shown to be likely to occur.

⁵ Ben Green, "The Responsible City: Avoiding Technology’s Undemocratic Social Contracts," *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future* (MIT Press, 2019), <https://smartenoughcity.mitpress.mit.edu/pub/yvyv9j2i>.

⁶ Toronto Waterfront Revitalization Corporation, Notice of Motion, (2020). par 30.

⁷ Toronto Waterfront Revitalization Corporation, *Notice of Motion*. par 31.

⁸ Toronto Waterfront Revitalization Corporation, *Notice of Motion*. par 32.

⁹ Toronto Waterfront Revitalization Corporation, *Notice of Motion*. par 39.

¹⁰ Green, "The Responsible City: Avoiding Technology’s Undemocratic Social Contracts."

¹¹ Green, "The Responsible City: Avoiding Technology’s Undemocratic Social Contracts."

¹² Bruce Schneier, "Data is a toxic asset, so why not throw it out?," *CNN* (2016), <http://www.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html> (Accessed April 28, 2020).

While it is true that the privacy harms listed in the Amended Notice of Application have yet to occur, there is little that is speculative about the claims made regarding the potential privacy harms of the Quayside project. A great deal of research and experience have demonstrated the significant privacy harms that are intertwined with any form of pervasive data collection, even when security and privacy measures such as de-identification are taken. This research was summarized in my first report and in the chapter “The Responsible City: Avoiding Technology’s Undemocratic Social Contracts” of my 2019 book *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*.¹³ My key concern is that large-scale data collection can allow for sensitive information to be revealed about individuals, even if each individual data point does not appear to do so. In addition, as described in my first report, pervasive data collection does not allow for people to give freely given, informed, specific, and unambiguous consent to data collection. In its own materials and presentations, Sidewalk Labs has acknowledged that “meaningful consent cannot be reasonably or reliably achieved” in public spaces.¹⁴

Based on the current state of knowledge regarding privacy in smart cities, there should be a strong presumption that instrumenting urban space with digital technology will result in privacy harms.¹⁵ With this in mind, I believe that the onus is on the organizations proposing such initiatives to proactively demonstrate that they have taken rigorous and comprehensive steps to prevent these privacy harms from occurring, based on the full range of policy, scientific, and technical knowledge about smart city privacy.

The recent documents from Waterfront Toronto and Sidewalk Labs do not demonstrate that the Quayside project is taking the necessary steps to avoid the variety of privacy harms associated with smart cities. Although both organizations state an interest in protecting privacy, the principles and intentions stated in these documents are far too vague to provide the necessary evidence that the project will not violate the public’s privacy. Even the Waterfront Toronto Digital Strategy Advisory Panel (DSAP) characterized the MIDP as “frustratingly abstract” and “overly focused on the ‘what’ rather than the ‘how.’”¹⁶

With initiatives like the Quayside project, the specific details are of great importance: in particular, precisely what data will be collected, how it will be stored, and how it will be used. Yet documents like the Waterfront Toronto Draft Digital Principles and Sidewalk Labs’ DIA continue to emphasize distinctions of data that do not align with scientific research. In particular, they emphasize de-identification as a viable privacy strategy, which has been well-documented for more than a decade as an insufficient privacy mechanism.

¹³ Green, “The Responsible City: Avoiding Technology’s Undemocratic Social Contracts.”

¹⁴ Sidewalk Labs, Digital Governance Proposals for DSAP Consultation, (2018), https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15_SWT_Draft+Proposals+Regarding+Data+Use+and+Governance.pdf?MOD=AJPERES, page 9.

¹⁵ Green, “The Responsible City: Avoiding Technology’s Undemocratic Social Contracts.”

¹⁶ Waterfront Toronto’s Digital Strategy Advisory Panel, DSAP Preliminary Commentary and Questions on Sidewalk Labs’ Draft Master Innovation and Development Plan (MIDP), (2019), https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/30c682ff-8172-49dc-bf63-09b2a2f1845a/DSAP+Preliminary+Commentary+-+September+10%2C+2019.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=30c682ff-8172-49dc-bf63-09b2a2f1845a, page 8.

The DIA divides data into four categories, based on sensitivity: non-personal data, aggregate data, de-identified data, and personal information. The DIA states, “the majority of services do not collect personal information. Moreover, the vast majority of data that would be created is non-personal, aggregate, or de-identified.”¹⁷ Although seemingly reassuring, the substance of these claims—based on the definitions of the key terms—is far less reassuring. The DIA states:¹⁸

- “De-identified data is data about an individual that was identifiable when collected but has subsequently been made non-identifiable.”
- “Non-personal data is data that does not identify an individual and can include other types of non-identifying data that is not about people.”
- “Personal information has a legal definition in Canada and is the subject of privacy laws, including the Personal Information Protection and Electronic Documents Act (PIPEDA).”

The definition of de-identified data is particularly concerning, as the DIA makes a false equivalence between “de-identified data” and “non-identifiable” data. As I described in my first report, de-identification is a poorly defined term and does not actually guarantee privacy or prevent the re-identification of individuals.¹⁹ This has been well known in the scientific and legal communities for more than a decade now. Consider, for example, the conclusions of the 2010 article “Myths and fallacies of personally identifiable information”:

“The versatility and power of re-identification algorithms imply that terms such as “personally identifiable” and “quasi-identifier” simply have no technical meaning. While some attributes may be uniquely identifying on their own, *any attribute can be identifying in combination with others*. [...] The emergence of powerful re-identification algorithms demonstrates not just a flaw in a specific anonymization technique(s), but the fundamental inadequacy of the entire privacy protection paradigm based on ‘de-identifying’ the data. De-identification provides only a weak form of privacy.”²⁰

The United States President’s Council of Advisors on Science and Technology (PCAST) similarly noted in 2014, “By data mining and other kinds of analytics, non-obvious and sometimes private information can be derived from data that, at the time of their collection, seemed to raise no, or only manageable, privacy issues. [...] one can never know what information may later be extracted from any particular collection of big data.”²¹ Waterfront Toronto’s Digital Strategy Advisory Panel has itself noted that “reliable de-identification is notoriously difficult to achieve.”²² The Office of

¹⁷ Sidewalk Labs, Master Innovation & Development Plan Digital Innovation Appendix, (2019), <https://quaysideto.ca/wp-content/uploads/2019/11/Sidewalk-Labs-Digital-Innovation-Appendix.pdf>. page 44.

¹⁸ Sidewalk Labs, *Master Innovation & Development Plan Digital Innovation Appendix*. page 49.

¹⁹ Green et al., "Open Data Privacy".

²⁰ Arvind Narayanan and Vitaly Shmatikov, "Myths and fallacies of personally identifiable information," *Communications of the ACM* 53, no. 6 (2010).

²¹ President’s Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective," (2014).

²² Waterfront Toronto’s Digital Strategy Advisory Panel, *DSAP Preliminary Commentary and Questions on Sidewalk Labs’ Draft Master Innovation and Development Plan (MIDP)*. page 18.

the Privacy Commissioner of Canada (OPC) has also noted, with regard to de-identification, that “there always remains a risk of re-identification.”²³

Re-identification is possible in large-scale datasets, despite each record potentially seeming benign in isolation, because it becomes possible to identify the unique patterns of individuals that are contained within these datasets.²⁴ Another cause for these concerns about re-identification is the mosaic effect, also described in more detail in my first report. The mosaic effect occurs when different datasets are combined to form a “mosaic” that identifies individuals and reveals private information from datasets that are each, on their own, de-identified and seemingly non-identifiable.²⁵ The mosaic effect further increases the difficulty of stating that data is “non-identifiable” or “non-personal”: even if those designations *did* accurately describe a dataset on its own, that does not guarantee that the data could not be combined with other data to become identifiable.

A great deal of scholarship and evidence underlines these concerns about re-identification. For example, in 2014, in response to a Freedom of Information Law (FOIL) request, New York City released data detailing every taxi ride recorded in registered NYC taxis during 2013.²⁶ The data was meant to be anonymized and contained information about pickup time and location, drop-off time and location, and the taxicab (in the form of license plate) and driver (in the form of medallion number) involved in each trip. By analyzing the destinations of all the trips leaving from a specific location, it was possible to identify the home addresses of several patrons of a Manhattan strip club.²⁷ Via the mosaic effect, it was possible to combine this information with other information that is available publicly online to identify the names of these patrons. Also through the mosaic effect, by combining that data with published paparazzi photos, a data scientist found that it was possible to identify where celebrities photographed getting into cabs were going.²⁸

Two studies further demonstrated the limits of de-identification by analyzing datasets that contained the mobile phone location traces²⁹ and credit card transactions³⁰ of more than one million people. Even though both datasets lacked direct identifiers (such as names)—the datasets included just a random number corresponding to each person as well as the locations and times that those people were tracked—it was possible to identify individuals and learn about their behavior. Remarkably, because the data contained precise information about each person’s distinct

²³ The Office of the Privacy Commissioner of Canada, “Consultation on the OPC’s Proposals for ensuring appropriate regulation of artificial intelligence,” (2020), https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/ (Accessed April 28, 2020).

²⁴ Yves-Alexandre de Montjoye et al., “Unique in the shopping mall: On the reidentifiability of credit card metadata,” *Science* 347, no. 6221 (2015).

²⁵ Green et al., “Open Data Privacy”.

²⁶ Chris Whong, “FOILING NYC’s Taxi Trip Data,” (2014), http://chriswhong.com/open-data/foil_nyc_taxi/ (Accessed April 28, 2020).

²⁷ Anthony Tockar, “Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset,” *Neustar Research* (2014), <https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/> (Accessed May 14, 2019).

²⁸ Tockar, “Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset”.

²⁹ Yves-Alexandre de Montjoye et al., “Unique in the Crowd: The privacy bounds of human mobility,” *Nature* 493, no. 7434 (2013).

³⁰ de Montjoye et al., “Unique in the shopping mall.”

patterns, more than 90 percent of people could be uniquely identified with just four data points of where they have been and when they were there.³¹

As such, treating de-identified data as “non-identifiable” assumes that this data is anonymous and more protected than it actually is, contradicting more than a decade of legal and technical scholarship on data privacy.

All told, this calls into question the DIA’s statement that “the majority of services do not collect personal information.”³² Personal information is defined by PIPEDA as “information about an identifiable individual.”³³ The DIA notes, “The broad legal definition of personal information includes any information that could be used, alone or in combination with other information, to identify an individual or that is associated with an identifiable individual”³⁴ and that “Information will be about an ‘identifiable individual’ where there is a possibility that an individual could be identified through the use of that information, alone or in combination with other information.”³⁵

Yet as I just described, de-identified data can often be linked back to an identifiable individual, whether on its own or through the mosaic effect. As the 2011 law review article “The PII Problem” writes, “whether information is identifiable to a person will depend upon context and cannot be pre-determined *a priori*.”³⁶ As such, it is not sufficient to limit “personal information” to attributes such as “age, name, ID numbers, income, ethnic origin, or blood type,” as the DIA does.³⁷ Instead, because it is clear when it comes to de-identified data that “there is a possibility that an individual could be identified through the use of that information, alone or in combination with other information,”³⁸ I believe that all of the “de-identified data” should be considered “personal information” under the DIA’s schema.

The entire framework of privacy and data governance rests on treating each category of data appropriately. Yet if the definitions of key categories overstate the level of privacy for that type of data, then the entire project is overstating the privacy associated with the collected data. Notably, the flaws in terms like “de-identification” have been known for many years: by 2010 research had clearly demonstrated these flaws, which have become only clearer and more pervasive in the ensuing years. Given this state of knowledge within privacy research, the DIA’s definitions for “de-identified” and related terms call into question the entire framework of privacy and data governance that Sidewalk Labs is proposing and that Waterfront Toronto is being asked to approve.

³¹ de Montjoye et al., “Unique in the Crowd.”; de Montjoye et al., “Unique in the shopping mall.”

³² Sidewalk Labs, *Master Innovation & Development Plan Digital Innovation Appendix*. page 44.

³³ “Personal Information Protection and Electronic Documents Act,” (2000), <https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/159208/sc-2000-c-5.html>

³⁴ Sidewalk Labs, *Master Innovation & Development Plan Digital Innovation Appendix*. page 49.

³⁵ Sidewalk Labs, *Master Innovation & Development Plan Digital Innovation Appendix*. page 271.

³⁶ Paul M. Schwartz and Daniel J. Solove, “The PII Problem: Privacy and a New Concept of Personally Identifiable Information,” *NYU Law Review* 86 (2011).

³⁷ Sidewalk Labs, *Master Innovation & Development Plan Digital Innovation Appendix*. page 271.

³⁸ Sidewalk Labs, *Master Innovation & Development Plan Digital Innovation Appendix*. page 271.

This issue of “de-identification” also calls into question the efficacy of “data minimization,” which is discussed in the DIA³⁹ and Draft Digital Principles.⁴⁰ Although data minimization is a good practice, the value of data minimization depends on *what data* is considered (to use language from the Draft Digital Principles describing data minimization) “necessary for the provision of identified and approved services that demonstrate benefit to individuals.”⁴¹ Given that the following bullet in the Draft Digital Principles is about “De-identification of personal data at source,” it would appear that data minimization is practiced to follow the standard of de-identification set forth in the DIA. If this is the case, then given what I have described above about the significant shortcomings of de-identification, the data that will be collected under this data minimization scheme will still represent highly invasive data collection that can be used to re-identify individuals.

Several recent articles further demonstrate the significant risks associated with initiatives involving any form of pervasive data collection.

In December 2019, the New York Times published a series of articles describing the information contained in a dataset of “more than 50 billion location pings from the phones of more than 12 million Americans as they moved through several major cities, including Washington, New York, San Francisco and Los Angeles.”⁴² The articles demonstrated how this information could be used to track the movements and behaviors of individuals without their knowledge or understanding, ranging from an average person all the way to President Donald Trump.⁴³

Notably, the New York Times obtained this data from an unauthorized source: a leak. As the articles describe:

The data was provided to Times Opinion by sources who asked to remain anonymous because they were not authorized to share it and could face severe penalties for doing so. The sources of the information said they had grown alarmed about how it might be abused and urgently wanted to inform the public and lawmakers. [...] Location data companies argue that your data is safe — that it poses no real risk because it’s stored on guarded servers. This assurance has been undermined by the parade of publicly reported data breaches — to say nothing of breaches that don’t make headlines. In truth, sensitive information can be easily transferred or leaked, as evidenced by this very story.⁴⁴

³⁹ Sidewalk Labs, *Master Innovation & Development Plan Digital Innovation Appendix*. pages 170, 226, 62-3, 73, 91-2.

⁴⁰ Waterfront Toronto, *Draft Digital Principles*, (2019), <https://quaysideto.ca/wp-content/uploads/2019/11/Final-Draft-Digital-Principles.pdf>. page 3.

⁴¹ Waterfront Toronto, *Draft Digital Principles*. page 3.

⁴² Stuart A. Thompson and Charlie Warzel, “Twelve Million Phones, One Dataset, Zero Privacy,” *The New York Times* (2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html> (Accessed April 28, 2020).

⁴³ Stuart A. Thompson and Charlie Warzel, “How to Track President Trump,” *The New York Times* (2019), <https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html> (Accessed April 28, 2020).

⁴⁴ Thompson and Warzel, “Twelve Million Phones, One Dataset, Zero Privacy”.

Whether through hacks, leaks, or sale, datasets collected by governments and companies often end up in unexpected and undesirable places.

Given that perfect security of existing datasets is impossible,⁴⁵ proper security requires collecting as little data as possible. The best way to secure data is to not collect it in the first place.

Data can end up in expected or undesirable hands not just through illicit leaks, but through data sharing that expands the use of information beyond its original scope and purpose. As part of a smart city program, San Diego has installed thousands of cameras and sensors into its streetlights. This technology was intended to reduce traffic—yet even after several years “it’s still unclear what the data will ultimately be used for.”⁴⁶ However, the video footage collected by the cameras has attracted the attention of local police, which (as of August 2019) had viewed this footage in relation to more than 140 cases. This is indicative of a broader pattern in smart cities: once data is collected—no matter the purpose—it is likely to expand the functional surveillance capabilities of law enforcement.⁴⁷ Whether it be traffic sensors, facial recognition technology,⁴⁸ corporate databases,⁴⁹ or cameras on doorbells,⁵⁰ data and video footage regularly end up being wielded by police to expand surveillance.

Even when a company makes promises about how it will protect privacy, it may not end up following through on those promises. A particularly salient example of this involves Google—the founder and now (under Alphabet) sister company of Sidewalk Labs—and DeepMind.⁵¹ When Google subsidiary DeepMind began working on health data from the UK National Health Service, DeepMind promised that this “data will never be connected to Google accounts or services.” In 2018, however, DeepMind Health was integrated into Google, making the two entities closely intertwined—precisely what DeepMind had previously promised would never occur. The company’s internal review board was also shut down at that time. Without a legal basis or mechanisms of enforcement, promises regarding how data will or will not be used may not be adhered to for very long. It is therefore insufficient for Sidewalk Labs and Waterfront Toronto to simply articulate promises about what practices they intend to follow; even if these practices were sufficient to protect privacy, the lack of legal enforcement ensuring that the principles are followed

⁴⁵ Shuman Ghosemajumder, “You Can’t Secure 100% of Your Data 100% of the Time,” *Harvard Business Review* (2017), <https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time> (Accessed April 28, 2020).

⁴⁶ Joshua Emerson Smith, “As San Diego increases use of streetlamp cameras, ACLU raises surveillance concerns,” *Los Angeles Times* (2019), <https://www.latimes.com/california/story/2019-08-05/san-diego-police-ramp-up-use-of-streetlamp-cameras-to-crack-cases-privacy-groups-raise-concerns> (Accessed April 28, 2020).

⁴⁷ Kate Crawford et al., “AI Now 2019 Report,” (2019), https://ainowinstitute.org/AI_Now_2019_Report.pdf

⁴⁸ Kashmir Hill, “The Secretive Company That Might End Privacy as We Know It,” *The New York Times* (2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> (Accessed April 28, 2020).

⁴⁹ Caroline Haskins, “300 Californian Cities Secretly Have Access to Palantir,” *Vice* (2019), https://www.vice.com/en_us/article/neaqq/300-californian-cities-secretly-have-access-to-palantir (Accessed April 28, 2020).

⁵⁰ Drew Harwell, “Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns,” *The Washington Post* (2019), <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true> (Accessed April 28, 2020).

⁵¹ Alex Hern, “Google ‘betrays patient trust’ with DeepMind Health move,” *The Guardian* (2018), <https://www.theguardian.com/technology/2018/nov/14/google-betrays-patient-trust-deepmind-healthcare-move> (Accessed April 28, 2020).

means that there is no guarantee that privacy will continue to be protected throughout the duration of the project.

Waterfront Toronto's position that the Amended Notice of Application is "premature" is also concerning given a statement made in the affidavit of Kristina Verner sworn January 17, 2020: that the organization has significant experience managing other "intelligent communities" projects.⁵² The experience listed is not sufficient to warrant the dismissal of privacy concerns regarding Quayside. Waterfront Toronto may have notable experience supporting the development of high-speed internet infrastructure, for example, but none of the experience entails the type of pervasive data collection and data governance required in Quayside. Indeed, the Auditor General of Ontario noted, "Up until the awarding of a project to Sidewalk Labs for the development of the smart city, Waterfront Toronto had primarily handled traditional mixed-use developments. As a result, it had limited experience in digital data infrastructure development."⁵³

As a result, I do not believe that the prior experiences that Ms. Verner lists provide evidence that Waterfront Toronto has relevant or sufficient experience with the privacy risks created by the Quayside project, nor with the governance mechanisms and processes required to manage those privacy risks. These projects do not provide evidence that Waterfront Toronto is equipped to manage the large-scale data collection, and associated privacy risks, that are proposed in the Quayside project.

In addition, the DIA introduces the notions of Software-Defined Networking (SDN) and Distributed Verifiable Credentials (DVCs). Although there may be other benefits to these approaches, they do not alter my conclusions regarding the privacy risks associated with the Quayside project. While these approaches may improve the security of data that is collected in Quayside and slightly reduce the amount of personal information that is collected, because they do not alter the broad scope or extent of data that is collected they do not alter my conclusions about the privacy risks of the Quayside project. Indeed, DSAP has noted that SDNs "pose privacy and surveillance risks that are ignored in Sidewalk's proposal"⁵⁴ and has questioned whether DVCs "fit within a project of this nature and scope"⁵⁵ and are "sufficiently established to depend on in the initial stages of Quayside development."⁵⁶ More broadly, privacy concerns such as those related to the Quayside project cannot be resolved through technical fixes alone, but instead require integrating technical approaches with law, governance, and attention to social context.⁵⁷

⁵² Verner, *Affidavit*, par 15.

⁵³ Office of the Auditor General of Ontario, "Section 3.15: Waterfront Toronto," *Annual Report 2018* (2018), https://www.auditor.on.ca/en/content/annualreports/arreports/en18/v1_315en18.pdf. page 689.

⁵⁴ Waterfront Toronto's Digital Strategy Advisory Panel, DSAP Supplemental Report on the Sidewalk Labs Digital Innovation Appendix (DIA), (2020), <https://quaysideto.ca/wp-content/uploads/2020/02/DSAP-Supplemental-Report-on-Sidewalk-Labs-Digital-Innovation-Appendix-DIA-Appendices-FINAL.pdf>. page 72.

⁵⁵ Waterfront Toronto's Digital Strategy Advisory Panel, *DSAP Supplemental Report on the Sidewalk Labs Digital Innovation Appendix (DIA)*. page 18.

⁵⁶ Waterfront Toronto's Digital Strategy Advisory Panel, *DSAP Supplemental Report on the Sidewalk Labs Digital Innovation Appendix (DIA)*. page 67.

⁵⁷ Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2009).

E. Conclusions

There is a vast weight of evidence regarding the risks of the data collection proposed in the Quayside project (and the likelihood of those harms arising). All told, these significant risks challenge the statement made by Kristina Verner in her January 17, 2020 affidavit that the MIDP is still “evolving” and so therefore should not be subject to litigation.⁵⁸ Indeed, Waterfront Toronto has already expressed support for 59 “digitally enabled solutions,”⁵⁹ suggesting that the project is taking an increasingly tangible and less-evolving form. Moreover, scholars of technology have long noted that the conception and architecture of technological systems significantly shape the social impacts of those technologies.⁶⁰ As noted above, a great deal of scholarship and journalism have demonstrated the close link between smart city style widespread data collection and privacy harms.⁶¹ As such, the broad strokes of the Quayside proposals—even if some specific details are still to be worked out—convince me that the Quayside project will introduce severe privacy risks with very likely privacy harms resulting. If such concerns related to privacy are allowed to bear weight only after the plans are finalized, then more often than not it is too late for those concerns to be meaningfully addressed.

F. References

- Crawford, Kate, Roel Dobbe, Theodora Dryer, Genevieve Fried, Ben Green, Elizabeth Kaziunas, Amba Kak, *et al.* "AI Now 2019 Report." (2019). https://ainowinstitute.org/AI_Now_2019_Report.pdf
- de Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. "Unique in the Crowd: The privacy bounds of human mobility." *Nature* *srep.* 3 (2013).
- de Montjoye, Yves-Alexandre, Laura Radaelli, Vivek Kumar Singh, and Alex “Sandy” Pentland. "Unique in the shopping mall: On the reidentifiability of credit card metadata." *Science* 347, no. 6221 (2015): 536-39.
- Ghosemajumder, Shuman. "You Can't Secure 100% of Your Data 100% of the Time." *Harvard Business Review* (2017). <https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time> (Accessed April 28, 2020).
- Green, Ben. "The Responsible City: Avoiding Technology's Undemocratic Social Contracts." In *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future* MIT Press, 2019. <https://smartenoughcity.mitpress.mit.edu/pub/yyvy9j2i>.
- Green, Ben. *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*. MIT Press, 2019.
- Green, Ben, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, and Susan Crawford. "Open Data Privacy: A risk-benefit, process-oriented approach to sharing and protecting municipal data." *Berkman Klein Center Research Publication* (2017). <http://nrs.harvard.edu/urn-3:HUL.InstRepos:30340010>

⁵⁸ Verner, *Affidavit*, par 6.

⁵⁹ Waterfront Toronto, Waterfront Toronto's MIDP Evaluation Consultation Discussion Guide, (2020), <https://quaysideto.ca/wp-content/uploads/2020/02/Quayside-Discussion-Guide-Round-Two-Consultation-February-18-2020.pdf>. page 9, 55-60.

⁶⁰ Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (University of Chicago Press, 1986).

⁶¹ Green, "The Responsible City: Avoiding Technology's Undemocratic Social Contracts."

- Hartzog, Woodrow. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Harvard University Press, 2018.
- Harwell, Drew. "Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns." *The Washington Post* (2019). <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true> (Accessed April 28, 2020).
- Haskins, Caroline. "300 Californian Cities Secretly Have Access to Palantir." *Vice* (2019). https://www.vice.com/en_us/article/neaqq/300-californian-cities-secretly-have-access-to-palantir (Accessed April 28, 2020).
- Hern, Alex. "Google 'betrays patient trust' with DeepMind Health move." *The Guardian* (2018). <https://www.theguardian.com/technology/2018/nov/14/google-betrays-patient-trust-deepmind-healthcare-move> (Accessed April 28, 2020).
- Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It." *The New York Times* (2020). <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> (Accessed April 28, 2020).
- Narayanan, Arvind, and Vitaly Shmatikov. "Myths and fallacies of personally identifiable information." *Communications of the ACM* 53, no. 6 (2010): 24-26.
- Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009.
- Office of the Auditor General of Ontario. "Section 3.15: Waterfront Toronto." In *Annual Report 2018/2019*. https://www.auditor.on.ca/en/content/annualreports/arreports/en18/v1_315en18.pdf.
- "Personal Information Protection and Electronic Documents Act." (2000). <https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/159208/sc-2000-c-5.html>
- President's Council of Advisors on Science and Technology. "Big Data and Privacy: A Technological Perspective." 2014.
- Schneier, Bruce. "Data is a toxic asset, so why not throw it out?" *CNN* (2016). <http://www.cnn.com/2016/03/01/opinions/data-is-a-toxic-asset-opinion-schneier/index.html> (Accessed April 28, 2020).
- Schwartz, Paul M., and Daniel J. Solove. "The PII Problem: Privacy and a New Concept of Personally Identifiable Information." *NYU Law Review* 86 (2011): 1814.
- Sidewalk Labs. *Digital Governance Proposals for DSAP Consultation*. 2018. https://waterfronttoronto.ca/nbe/wcm/connect/waterfront/41979265-8044-442a-9351-e28ef6c76d70/18.10.15_SWT_Draft+Proposals+Regarding+Data+Use+and+Governance.pdf?MOD=AJPERES.
- Sidewalk Labs. *Master Innovation & Development Plan Digital Innovation Appendix*. 2019. <https://quaysideto.ca/wp-content/uploads/2019/11/Sidewalk-Labs-Digital-Innovation-Appendix.pdf>.
- Smith, Joshua Emerson. "As San Diego increases use of streetlamp cameras, ACLU raises surveillance concerns." *Los Angeles Times* (2019). <https://www.latimes.com/california/story/2019-08-05/san-diego-police-ramp-up-use-of-streetlamp-cameras-to-crack-cases-privacy-groups-raise-concerns> (Accessed April 28, 2020).
- The Office of the Privacy Commissioner of Canada. "Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence." (2020).

- https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/ (Accessed April 28, 2020).
- Thompson, Stuart A., and Charlie Warzel. "How to Track President Trump." *The New York Times* (2019). <https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html> (Accessed April 28, 2020).
- Thompson, Stuart A., and Charlie Warzel. "Twelve Million Phones, One Dataset, Zero Privacy." *The New York Times* (2019). <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html> (Accessed April 28, 2020).
- Tockar, Anthony. "Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset." *Neustar Research* (2014). <https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/> (Accessed May 14, 2019).
- Toronto Waterfront Revitalization Corporation. *Notice of Motion*. 2020.
- Verner, Kristina Lynna. *Affidavit*. 2020.
- Waterfront Toronto. *Draft Digital Principles*. 2019. <https://quaysideto.ca/wp-content/uploads/2019/11/Final-Draft-Digital-Principles.pdf>.
- Waterfront Toronto. *Waterfront Toronto's MIDP Evaluation Consultation Discussion Guide*. 2020. <https://quaysideto.ca/wp-content/uploads/2020/02/Quayside-Discussion-Guide-Round-Two-Consultation-February-18-2020.pdf>.
- Waterfront Toronto's Digital Strategy Advisory Panel. *DSAP Preliminary Commentary and Questions on Sidewalk Labs' Draft Master Innovation and Development Plan (MIDP)*. 2019. https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/30c682ff-8172-49dc-bf63-09b2a2f1845a/DSAP+Preliminary+Commentary+-+September+10%2C+2019.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=30c682ff-8172-49dc-bf63-09b2a2f1845a.
- Waterfront Toronto's Digital Strategy Advisory Panel. *DSAP Supplemental Report on the Sidewalk Labs Digital Innovation Appendix (DIA)*. 2020. <https://quaysideto.ca/wp-content/uploads/2020/02/DSAP-Supplemental-Report-on-Sidewalk-Labs-Digital-Innovation-Appendix-DIA-Appendices-FINAL.pdf>.
- Whong, Chris. "FOILing NYC's Taxi Trip Data." (2014). http://chriswhong.com/open-data/foil_nyc_taxi/ (Accessed April 28, 2020).
- Winner, Langdon. *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. University of Chicago Press, 1986.

ONTARIO
SUPERIOR COURT OF JUSTICE
(DIVISIONAL COURT)

BETWEEN:

CORPORATION OF THE CANADIAN CIVIL LIBERTIES ASSOCIATION and
 LESTER BROWN

Applicants

and

TORONTO WATERFRONT REVITALIZATION CORPORATION, CITY OF
 TORONTO, HER MAJESTY IN RIGHT OF ONTARIO as represented by the
 MINISTER OF INFRASTRUCTURE, HER MAJESTY IN RIGHT OF CANADA as
 represented by the MINISTER OF COMMUNITIES AND INFRASTRUCTURE, AND
 THE ATTORNEY GENERAL OF CANADA

Respondents

APPLICATION under sections 2 and 6(1) and 6(2) of the *Judicial Review Procedure Act*, R.S.O. 1990, c. J.1, as amended, and sections 2, 7, 8 and 24 of the *Charter of Rights and Freedoms*.

ACKNOWLEDGMENT OF EXPERT'S DUTY

1. My name is Ben Green. I live in New York City in the state of New York.
2. I have been engaged by or on behalf of the Corporation of the Canadian Civil Liberties Association and Lester Brown to provide evidence in relation to the above-noted court proceeding.
3. I acknowledge that it is my duty to provide evidence in relation to this proceeding as follows:
 - (a) to provide opinion evidence that is fair, objective and non-partisan;
 - (b) to provide opinion evidence that is related only to matters that are within my area of expertise; and
 - (c) to provide such additional assistance as the court may reasonably require, to determine a matter in issue.
4. I acknowledge that the duty referred to above prevails over any obligation which I may owe to any party by whom or on whose behalf I am engaged.

Signature 

Date: April 29, 2020

CORPORATION OF THE CANADIAN CIVIL LIBERTIES
ASSOCIATION et al.
Applicants

-and- TORONTO WATERFRONT REVITALIZATION CORPORATION et
al.
Respondents

Court File No. 211/19

**ONTARIO
SUPERIOR COURT OF JUSTICE
(DIVISIONAL COURT)**

PROCEEDING COMMENCED AT
TORONTO

**ACKNOWLEDGMENT OF EXPERT'S DUTY OF
BEN GREEN**

FOGLER, RUBINOFF LLP

Lawyers
77 King Street West
Suite 3000, P.O. Box 95
TD Centre North Tower
Toronto, ON M5K 1G8

Young Park (LSO# 43550E)

Tel: 416.365.3727
Fax: 416.941.8852
ypark@foglers.com

Robert B. Macdonald (LSO# 60512B)

Tel: 647.729.0754
Fax: 416.941.8852
rmacdonald@foglers.com

Lawyers for the Applicants

Ben Green

Harvard University
Maxwell Dworkin 209
33 Oxford St, Cambridge, MA 02138

Phone: (617) 413-0594
Email: bgreen@harvard.edu
Site: <http://scholar.harvard.edu/bgreen>

INTERESTS	Data, algorithms, and social justice Municipal governance of technology	
AFFILIATIONS	Berkman Klein Center for Internet & Society at Harvard Affiliate Fellow	2018 – Present 2016 – 2018
EDUCATION	Harvard University PhD in Applied Mathematics MS in Applied Mathematics	2020 (expected) 2016
	Yale University BS in Mathematics & Physics, with distinction (Cum Laude)	2014
GRANTS	Berkman Klein Center for Internet & Society Fellowship Harvard Kennedy School Taubman Center Urban Experience Fellowship NSF Graduate Research Fellowship DOD National Defense Science and Engineering Graduate Fellowship (declined) Herbert Winokur SEAS Graduate Fellowship Eric & Wendy Schmidt Data Science for Social Good Summer Fellowship Dwight Hall at Yale Urban Fellowship New Haven Mayor's Community Arts Grant Yale President's Public Service Fellowship Alan S. Tetelman 1958 Fellowship for International Research in the Sciences	2016 2016 2015 2015 2015 2014 2013 2013 2013 2011
BOOKS	Ben Green. <i>The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future</i> . MIT Press. (2019).	
PAPERS	Ben Green and Yiling Chen. "Disparate Interactions: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments." <i>ACM Conference on Fairness, Accountability, and Transparency (ACM FAT*)</i> (2019). Best Technical and Interdisciplinary Paper	
	Ben Green. "'Fair' Risk Assessments: A Precarious Approach for Criminal Justice Reform." <i>5th Workshop on Fairness, Accountability, and Transparency in Machine Learning (ICML)</i> (2018).	
	Ben Green and Lily Hu. "The Myth in the Methodology: Towards a Recontextualization of Fairness in Machine Learning." <i>Machine Learning: The Debates Workshop (ICML)</i> (2018).	
	Ben Green, Thibaut Horel, and Andrew Papachristos. "Modeling contagion through social networks to explain and predict gunshot violence in Chicago, 2006 to 2014." <i>JAMA Internal Medicine</i> 177, no. 3 (2017): 326–333.	
	Ben Green, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, and Susan Crawford. "Open Data Privacy: A risk-benefit, process-oriented approach to sharing and protecting municipal data," <i>Berkman Klein Center Research Publication</i> (2017).	
	Ben Green, Paul Bardunias, J. Scott Turner, Radhika Nagpal, and Justin Werfel. "Excavation and aggregation as organizing factors in de novo construction by mound-building termites." <i>Proceedings of the Royal Society B</i> 284, no. 1856 (2017).	

Ben Green, Alejandra Caro, Matt Conway, Robert Manduca, Tom Plagge, and Abby Miller. "Mining administrative data to spur urban revitalization." *Proceedings of the 21st ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)* (2015).

Ben Green. "Testing and quantifying collective intelligence," *Proceedings of the Collective Intelligence Conference* (2015).

SELECTED TALKS

- 2019
 MIT Press Bookstore
 MIT Department of Urban Studies and Planning
 Harvard Institute for Learning in Retirement
 Carleton University Master of Public Policy and Administration program
 Harvard Applied Computation 221: Critical Thinking in Data Science (guest lecture)
 Seton Hall University Law School Institute for Privacy Protection Spring Conference
 University of California, Irvine
 Harvard Sociology 98AB: Urban Politics in the Global City (guest lecture)
 Berkman Klein Center Luncheon Series
 ACM FAT*
 Crime Lab New York
 AI Now Institute, NYU
- 2018
 Strategic Leadership Development for Senior Vietnamese Government Officials
 MetroLab Annual Summit (panel moderator)
 University of Indiana Ostrom Workshop on Smart Cities
 Privacy Task Force for New Jersey Municipalities
 FATML (ICML workshop)
 Machine Learning: The Debates (ICML workshop)
 Humboldt University of Berlin Faculty of Law
 Boston City Council (invited expert testimony)
 Berkman Klein Center Attorney General Tech Forum
 Seton Hall Law School Artificial Intelligence and the Law Conference
- 2017
 Seton Hall Law School Institute for Privacy Protection Conference on New and Nontraditional Actors in Privacy and Social Media Regulation
 Cambridge City Council (invited expert testimony)
 National Network for Safe Communities National Conference
 Harvard Data Privacy Lab Talks on Technology Science
 LibrePlanet
 Boston Area Research Initiative Spring Conference
 Future of Privacy Forum Smart Cities working group
- 2016
 City of Cambridge Open Data Review Board
 Digital Communities Mid-Year CIO Leadership Group Meeting
- 2015
 KDD
 Collective Intelligence

RESEARCH EXPERIENCE

- Harvard University**
Computer Science Department Graduate research assistant
Criminal justice algorithms September 2017 – Present
 Studying the social impacts of risk assessments in the criminal justice system.
- Berkman Center for Internet & Society** Data governance fellow
Best practices for municipal data governance January 2016 – August 2017
 Developed best practices for how cities manage data and technology. Studied the privacy

implications behind open data and developing a framework for assessing privacy risks when sharing data. Provided resources for cities to protect against discrimination when making data-driven decisions. Regularly convened with and presented to municipal leaders.

Yale University

Sociology Department

Gun violence in co-offending networks

Research assistant
January 2014 – January 2017

Studied the structure of criminal networks in eight American cities and identified risk factors for gunshot victims. Analyzed police records on arrests and shootings to model the diffusion of gun violence as an epidemic that spreads from person to person via social interactions. Developed a predictive model for who is at risk to be shot that outperforms traditional approaches.

Harvard University

Computer Science Department

Collective intelligence in termite colonies

Graduate research assistant
September 2014 – May 2016

Studying collective intelligence in termite colonies to determine how termites self-organize to collectively construct mounds. Designed experiments and conducted field research in Namibia. Developed simulations to infer the social dynamics in self-organizing groups of termites.

The Eric & Wendy Schmidt

Data Science for Social Good

Summer Fellowship

Data mining for urban revitalization

Research fellow
June 2014 – August 2014

Worked with the Mayor's Innovation Team in Memphis, TN to identify data-driven strategies for urban revitalization. Developed a machine learning classifier and interactive website to help policymakers and developers identify distressed houses in Memphis.

Yale University

Physics Department

Improved sampling of galaxy clustering

Undergraduate senior thesis
September 2013 – May 2014

Analyzed and developed algorithms and statistical methods to produce accurate sampling of galaxy clusters for the Dark Energy Spectroscopic Instrument.

Yale University

Mechanical Engineering Department

Emergent group behavior of insect swarms

Research assistant
September 2013 – January 2014

Studied the emergent behavior and complex dynamics of insect swarms. Used network applications to analyze the interactions between pairs of insects.

CERN

Statistical tests to detect elementary particles

Research assistant
May 2011 – July 2011

Worked on the ATLAS experiment of the Large Hadron Collider. Analyzed decay patterns of top quarks to search for a Z boson outside of the Standard Model. Conducted statistical analyses of particle collisions, comparing Monte Carlo simulations with recorded ATLAS data.

**PROFESSIONAL
EXPERIENCE**

City of Boston

Department of Innovation & Technology

Municipal data analytics and policy

Data analytics fellow
June 2016 – May 2017

Worked for the Citywide Analytics Team analyzing data and developing policies to aid City Departments improve operations and services. Analyzed Fire Department and EMS responses and made recommendations for process improvements, including a pilot program that pairs public health and medical resources to respond to certain incidents. Aided in the development of policies and practices for a new open data portal.

City of New Haven

Department of Transportation

Improving transportation efficiency and safety

Policy intern
May 2013 – May 2014

Analyzed New Haven's on-street parking regulations and made changes in order to reduce con-

gestion and aid economic development. Coordinated adoption of cellphone payment technology in meters throughout the city. Conceived and initiated process of creating a traffic garden for New Haven. Wrote pedestrian and bicycle safety guides.

Design for America at Yale

Creating artistic bike racks

Created a team to promote a more sustainable cycling environment in New Haven. Initiated and ran a program matching local artists and businesses to create three downtown bike racks that double as public art. Received a 2013 New Haven Mayor's Community Arts Grant to fund artistic bike racks throughout New Haven.

Team founder and leader

September 2012 – May 2014

Litl, Inc.

Machine learning for computer vision

Developed machine learning and computer vision algorithms for the photo-viewing application Woven. Developed a classifier to determine whether a picture was taken indoors or outdoors. Used techniques such as logistic regression, graph clustering, and Bayesian analysis.

Research and development intern

May 2012 – August 2012

TEACHING

Faculty member, UC Irvine Technology, Law, and Society Summer Institute, June 2018.
Course assistant, Harvard Law School Responsive Communities Lab, Fall 2016.
Head teaching fellow, Harvard Computer Science 182: Artificial Intelligence, Fall 2015.
Math and science coordinator, Dwight Hall Academic Mentoring Program at Yale.
Tutor, Yale College Science and Quantitative Reasoning Center.

SERVICE

Program Committee: Black in AI (NeurIPS workshop) 2018; Conference on Fairness, Accountability, and Transparency (FAT*) 2019, International ACM Web Science Conference (WebSci) 2019, Debugging Machine Learning Models (ICLR workshop) 2019, Mechanism Design for Social Good (EC workshop) 2019
Reviews: MIT Press (3x); Big Data & Society; Online Information Review; Data Mining and Knowledge Discovery; npj Digital Medicine
Institutional: Harvard Graduate Student Union Bargaining Committee Member

CORPORATION OF THE CANADIAN CIVIL LIBERTIES
ASSOCIATION et al.
Applicants

-and- TORONTO WATERFRONT REVITALIZATION
CORPORATION et al.
Respondents

Court File No. 211/19

**ONTARIO
SUPERIOR COURT OF JUSTICE
(DIVISIONAL COURT)**

PROCEEDING COMMENCED AT
TORONTO

AFFIDAVIT OF BEN GREEN

FOGLER, RUBINOFF LLP

Lawyers

77 King Street West

Suite 3000, P.O. Box 95

TD Centre North Tower

Toronto, ON M5K 1G8

Young Park (LSO# 43550E)

Tel: 416.365.3727

Fax: 416.941.8852

ypark@foglers.com

Robert B. Macdonald (LSO# 60512B)

Tel: 647.729.0754

Fax: 416.941.8852

rmacdonald@foglers.com

Lawyers for the Applicants