

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, Ellen P. Goodman, of the City of Philadelphia, in the State of Pennsylvania, in the United States of America, MAKE OATH AND SAY:

1. I am a Professor of law at Rutgers University and the Co-Director of the Rutgers Institute for Information Policy & Law. I research, teach and publish in the areas of information law, policy and digital governance, digital infrastructure and data analytics at the local level. Before joining Rutgers faculty, I was a partner in the Washington, D.C. law firm of Covington & Burling LLP from 2000 to 2002 and served as Of Counsel with the firm from 2002 to 2009. Prior to that, I clerked for Judge Norma L. Shapiro on the U.S. Federal District Court for the Eastern District of Pennsylvania, after graduating from Harvard Law School

E/G

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.
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 of the City of Philadelphia, in the State of Pennsylvania, to the Town of Oakville, in the Province of Ontario, On April 30<sup>th</sup> 2020.



Commissioner for Taking Affidavits  
(or as may be)

YOUNG PARK / LSO# 43550E



Ellen Goodman



This is Exhibit "1" referred to in the Affidavit of Ellen P. Goodman sworn April 30, 2020.

  
\_\_\_\_\_  
*Commissioner for Taking Affidavits (or as may be)*

YOUNG PARK

Expert Opinion prepared by Professor Ellen P. Goodman  
for Fogler Rubinoff in connection with CCLA Project

### **Abstract**

Waterfront Toronto is supporting 144 of 160 technologies that Sidewalk Labs has proposed for a new Quayside neighborhood. These technologies are meant to be essential infrastructure running much of what happens in a city, including housing, transit, energy, and sanitation. At the same time, Waterfront Toronto has acknowledged that there is inadequate public control over how these technologies are deployed. How much data, and of what sort, will be collected and used is still unknown. How Sidewalk and other vendors will monetize the data – assuming they will -- is unknown. Nor is it clear how people in Quayside can meaningfully withhold consent to data collection and use when they lack practical alternatives to obtain necessary services.

Waterfront Toronto's response to these concerns, thus far, is twofold: (1) Sidewalk Labs promises that it will adopt best digital governance practices; and (2) the Project can be adapted to digital governance mechanisms as they come into being. Neither of these responses is adequate to safeguard the privacy interests and secure the consent of the people of Quayside who will be subjected to novel surveillance technologies and participating in the algorithmic production of novel data derivatives. Companies often alter their commitments when needs and circumstances change, as is well documented in the recent history of technology roll-outs. Even more significant is path dependency on technology. Especially once built into fixed infrastructure like roads and utilities, the proposed technologies may not be easily reconfigured. While it may be years before ground is broken in Quayside, it will not be too long before contracts are executed and permits sought. If the digital governance comes only then, it will probably be too late to change course.

This report details ways in which Sidewalk Lab's assurances and Waterfront Toronto's wait-and-see approach fail to mitigate specific privacy threats. These threats include the excessive collection and use of personal information, excessive faith in data de-identification, inadequacy of user notice and consent, potential monetization of data derivatives, and integration of other Alphabet company data into Quayside applications. These threats are not speculative, but have all materialized in other deployments of digital technologies in similar contexts. Technology companies have broken promises about data collection and sharing, have changed terms-of-service in ways that vitiate consumer consent, and have added surveillance capabilities to services that were not originally expected to perform those functions. In all these cases, it has proven difficult for regulators and courts to remedy the privacy violations after the fact.

### **Expertise**

I teach and research in the area of information policy, law, and digital governance, focusing especially on digital infrastructure and data analytics at the local level. The courses I teach

include privacy, artificial intelligence, media, copyright, and property law. Relevant recent articles include: *Smart City Ethics*, in Oxford Handbook of the Ethics of Artificial Intelligence (forthcoming 2020), *Information Fidelity*, NEVADA L. REV. (forthcoming 2020), *Urbanism Under Google: Lessons from Sidewalk Toronto*, 88 FORDHAM L. REV. 457 (2019) (with Julia Powles), *Defining Equity in Algorithmic Change*, REGULATORY REVIEW (2019), *Report of the Media Subcommittee for the Study of Digital Platforms*, George J. Stigler Center for the Study of the Economy and the State The University of Chicago Booth School of Business (2019) (co-author), *Algorithmic Transparency for the Smart City*, 20 YALE J. OF LAW & TECH. 103 (2018) (with Robert Brauneis), *Zero Rating Broadband Data: Equality and Free Speech at the Network's Other Edge*, 15 COLO. TECH. L. J 63 (2016), *The Atomic Age of Data: Policies for the Internet of Things*, Aspen Institute Report (2015), *"Smart Cities" Meet Anchor Institutions: Public Libraries and Broadband*, 41 FORDHAM URBAN L. J. 1665 (2014).

My CV is attached.

### What I Reviewed

Prior to being engaged in this matter, I co-wrote an article on the first eighteen months of the Waterfront Toronto – Sidewalk Labs Quayside Project (the “Project”) and reviewed many of the most important documents available through 2018. That article, co-written with Dr. Julia Powles, is *Urbanism Under Google: Lessons from Sidewalk Toronto*, 88 Fordham L. Rev. 457 (2019).<sup>1</sup>

In connection with this matter, I reviewed the following:

- The Amended Notice of Application, April 16, 2019;
- The Affidavit of Kristina Lynne Verner, sworn Jan. 17, 2020;
- The Affidavit of Ben Green, sworn May 24, 2019;
- The Affidavit of Zeynep Tufekci, sworn June 4, 2019;
- The Sidewalk Labs Master Innovation and Development Plan, June 17, 2019;
- The Digital Strategy Advisory Panel (DSAP) Preliminary Commentary and Questions on Sidewalk Labs’ Draft Master Innovation and Development Plan, Aug. 19, 2019;
- The Waterfront Toronto Threshold Issues Resolution letter, Oct. 31, 2019;
- The Sidewalk Labs Digital Innovation Appendix, Nov. 14, 2019;
- Waterfront Toronto’s MIDP Evaluation Consultation February 2020, Round 2 Discussion Guide, Feb. 19, 2020; and
- The DSAP Supplemental Report on the Sidewalk Labs Digital Innovation Appendix, Feb. 26, 2020.

---

<sup>1</sup> Available at <https://ir.lawnet.fordham.edu/flr/vol88/iss2/4>.

## Questions Posed

I have been asked to address the following questions:

Do the documents you have examined from Sidewalk Labs and Waterfront Toronto disclose a digital governance regime that:

(A) is adequate to secure consent from and protect the privacy of people within Quayside?

(B) accounts for flaws known to have led to privacy and security breaches in the past?

## Summary of Opinion

In my article on the initial stages of the Project, I documented how the partnership between Waterfront Toronto (“WT”) and Sidewalk Labs (“Sidewalk”) as intended Project co-planners lacked a public-first approach to digital governance. The entity to be governed – often Sidewalk – is also positioned as the governor. The Project is structured such that it is Sidewalk that decides in the first instance what data will be collected, how it will be used, and whether people may opt out, without being bound by clear public policy on urban data flows. WT’s Digital Strategy Advisory Panel (“DSAP”), in its review of the Master Innovation & Development Plan (“MIDP”) and the Digital Innovation Appendix (“DIA”), repeatedly expressed concern about the absence of pre-approval digital governance frameworks.

Sidewalk’s role as digital architect means that it will indelibly shape the Project’s data flows, even if public governance comes later. Sidewalk promises to protect the public interest while at the same time fulfilling its obligations to shareholders, leaving reconciliation of these objectives to future public enforcement of as yet un-enacted rules. The cascading provisionality of privacy protections is particularly concerning because of the history of Sidewalk’s parent company, Alphabet, with respect to privacy-related commitments. The Project necessarily rests on contingent vows to unknown governance principles that may never be implemented or implementable once the technologies are baked into a new neighborhood plan.

Part I of this report describes how weaknesses in the Project’s digital governance will likely compromise privacy protections in a future Quayside neighborhood. Parts II and III address the two specific questions posed. Part II examines how the Project’s proposed technologies – looking at a few – cannot be expected to protect privacy and secure the consent of the people in Quayside. Part III examines how past projects of Alphabet’s and other technology companies counsel skepticism about relying on their promises in lieu of robust public governance.

## I. Digital Governance and the Project

Digital governance refers to how digital technologies, including the data flows they generate and use, are organized to achieve particular goals like privacy. In the context of this opinion, the question is whether the digitally-enabled portions of the Project are subject to controls sufficient to protect the privacy and secure the consent of the people within Quayside. The short answer is that they are not. Many of the controls that Sidewalk and WT gesture towards are prospective, their shape and application unknowable. WT's assessment of the adequacy of digital governance rests on Sidewalk's own definition of the problem and its proposed solutions, leading to the substitution of a vendor's judgment for public administration. These governance deficiencies will be baked into the Project as a whole, not only the specific technologies addressed in Part II below.

### A. Sidewalk's Promises are Not a Substitute for Public Digital Governance

WT's apparent reliance on Sidewalk's promises of self-regulation and compliance with future public policy does not adequately safeguard the public interest in data flows, because both the policies and enforcement mechanisms are unknown. Kristina Verner, Vice-President, Innovation, Sustainability and Prosperity at WT, stated in her Affidavit of Jan. 17, 2020, that the Project's "concepts are constantly evolving, adapting, and improving and the specifics of digital and privacy matters are not yet identified."<sup>2</sup> Slightly over one month later, WT issued guidance supporting 90% of Sidewalk's "proposed solutions" and 100% of those solutions that are "digitally enabled." In doing so, it recognized that WT might not "have sufficient controls in place to address the risks associated with the implementation of this project and partner," but that resolution of this concern would be "subject to commercial negotiations with Sidewalk Labs."<sup>3</sup>

To the extent that contract is serving as a proxy for public governance, it is important to note what Sidewalk is promising. As part of the Threshold Issues Resolution letter, the company committed to adhere "to all current and future Canadian privacy and data protection laws, regulations, and Waterfront Toronto's Digital Principles."<sup>4</sup> These Principles refer to the five "Working Principles"<sup>5</sup> at the heart of the forthcoming City of Toronto's "comprehensive Digital Infrastructure Plan (DIP) that will serve as an evaluation tool for external proposals with digital

---

<sup>2</sup> The Affidavit of Kristina Lynne Verner, sworn Jan. 17, 2020, at para 79 ("Verner Affidavit").

<sup>3</sup> Waterfront Toronto Threshold Issues Resolution letter (Oct. 32, 2019). *See also* Waterfront Toronto's MIDP Evaluation Consultation February 2020, Round 2 Discussion Guide ("WT Round 2 Discussion Guide") at 3, [https://quaysideto.ca/wp-content/uploads/2020/02/Quayside-Discussion-Guide-Round-Two-Consultation-February-18-2020.pdf?utm\\_source=The+Logic+Master+List&utm\\_campaign=748aa2ae60-Daily+Briefing+2020+Feb18+1&utm\\_medium=email&utm\\_term=0\\_325d5d3b52-748aa2ae60-275620453](https://quaysideto.ca/wp-content/uploads/2020/02/Quayside-Discussion-Guide-Round-Two-Consultation-February-18-2020.pdf?utm_source=The+Logic+Master+List&utm_campaign=748aa2ae60-Daily+Briefing+2020+Feb18+1&utm_medium=email&utm_term=0_325d5d3b52-748aa2ae60-275620453)

<sup>4</sup> *See* WT Round 2 Discussion Guide.

<sup>5</sup> The Principles are at a high level of abstraction: Equity and Inclusion; A Well-run City; Social, Economic and Environmental Benefits; Privacy and Security; Democracy and Transparency.

elements, such as those related to Quayside.”<sup>6</sup> In addition to the inchoate DIP, WT is apparently working on Intelligent Community Guidelines (ICG).

Since neither the DIP nor the ICG existed when the MIDP was created – nor do they exist yet – the MIDP is not governed by these regimes. Instead, the MIDP and later clarifying documents anticipate some future digital governance regime that, it is hoped, the then-embedded technologies can be adapted to. As the DSAP observes, this governance “framework has (potentially significant) gaps, especially in enforcement.”<sup>7</sup> Substantive standards are still in the offing and there is no method for operationalizing them through monitoring, oversight, and enforcement.

In addition to whatever Sidewalk contractually commits to, WT says the city permitting process can bind the company to certain digital governance promises; it does not say how other promises will be enforced. To be more specific, the set of promises that WT relies on appear to be: Sidewalk’s compliance with the forthcoming ICG; Sidewalk’s promised compliance with Toronto’s Digital Principles; Sidewalk’s promise not to sell personal information, use it for advertising, or share it without explicit consent; Sidewalk’s promise to ensure resilience and security for digital systems and infrastructure through prevention, detection, and rapid restoration; Sidewalk’s promise to use its own internal accountability mechanisms, including Responsible Data Use Guidelines and Responsible Artificial Intelligence (AI) Principles; and Sidewalk’s proposed development of physical systems (e.g., Super-PON, Koala mounts, Software-defined networking) to manage data flows.<sup>8</sup>

The MIDP itself acknowledges that more digital governance will be needed to ensure that Quayside’s digitally-enabled infrastructure does not collect more data than necessary, that data flows will be in the public interest, and that people in Quayside will have appropriate control over data flows, among other goals. That is why the MIDP proposed a range of new governance bodies, including the Urban Data Trust, earlier called the Civic Data Trust.<sup>9</sup> These governance proposals met with strong opposition and Sidewalk decided to drop them.<sup>10</sup> But nothing new has been adopted or even proposed to take their place. Notably, no relevant governmental, or other publicly accountable, entity has yet enacted governance regimes or mechanisms to

---

<sup>6</sup> City of Toronto, <https://www.toronto.ca/city-government/planning-development/waterfront/initiatives/current-projects/quayside/>. See also Letter from Kristina Verner, Vice President, Innovation, Sustainability, and Prosperity, Waterfront Toronto to Michael Geist, Digital Strategy Advisory Panel, Feb. 26, 2020 (“The City of Toronto is actively working on its Digital Infrastructure Plan, the Province on its Data Strategy, and the Government of Canada on PIPEDA and a Digital Charter”), <https://quaysideto.ca/wp-content/uploads/2020/02/Waterfront-Toronto-Response-to-DSAP-Supplemental-Report-on-the-Sidewalk-Labs-Digital-Innovation-Appendix-DIA.pdf>.

<sup>7</sup> DSAP Supplemental at 11-12.

<sup>8</sup> MIDP, Volume 2 at 32-189.

<sup>9</sup> MIDP, Volume 2 at 414-423. The proposal originated in Sidewalk Labs, Digital Governance Proposal 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](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).

<sup>10</sup> DIA at 225 (“Further to feedback on the data governance aspects of the proposal, Sidewalk Labs and Waterfront Toronto have agreed not to pursue establishing the Urban Data Trust as a new entity for this project”).



control data flows. For now, Sidewalk has proposed to rely on its draft Responsible Data Use Guidelines.<sup>11</sup> As the DSAP notes, this amalgam of private commitments and future policies does not amount to “a fully realized digital governance framework.”<sup>12</sup> In short, the governance gap that Sidewalk itself recognized in the MIDP has not been filled.<sup>13</sup>

Promises to self-regulate must be viewed with skepticism especially because of the way technology companies have expanded their data collection and use practices. Examples are in Part III below. With respect to enforcement-by-contract, cities like New York have had difficulty holding smart city vendors to their franchise agreements. For example, Intersection (one of Sidewalk’s investments) has reportedly failed to install the number of WiFi kiosks it promised and to pay the city what its franchise agreement requires, as discussed in Part III below. New York officials have lodged their complaints and lawsuits may follow, but the fact is that a city’s ability to enforce vendor agreements is not always robust.

The experiences of several American cities with Google Fiber installations provide another cautionary tale of unfounded reliance on vendor promises, especially when the company changes course. Google Fiber, another Alphabet entity, sold cities on the idea that it would make high-speed broadband much more affordable and accessible. But when infrastructure costs mounted, Google Fiber scaled back its ambitions.<sup>14</sup> A newspaper editorial in Kansas City – the first city to contract with Google Fiber – lamented: “Google Fiber hasn’t changed the world, or even this part of it. That will be worth remembering the next time an amazing technology emerges from Silicon Valley.”<sup>15</sup> The experience in Louisville Kentucky is perhaps even more relevant. There, Google Fiber engineered city regulations in its favor and even got the city to push for favorable federal regulation. But when the economics didn’t work out, the company left the city, even leaving its fiber cables exposed on city streets.<sup>16</sup> The point is not that the

---

<sup>11</sup> DIA at 225-226.

<sup>12</sup> DSAP Supplemental at 3.

<sup>13</sup> Rohit T. (“Rit”) Aggarwala, Sidewalk Labs’ Head of Urban Systems, also recognized the governance gaps in an interview with the BBC World Service’s Business Daily: “In the absence of a legal framework for what is and is not an acceptable thing to do with information, everything is subject to the policies and decisions by companies.” See BBC World Service, Smart cities: Big Data’s watching you (Oct. 24, 2019), <https://www.bbc.co.uk/sounds/play/w3csy7f9> (“Aggarwala interview”).

<sup>14</sup> Susan Crawford, Google Fiber Was Doomed From the Start, Wired (Mar. 14, 2017), <https://www.wired.com/2017/03/google-fiber-was-doomed-from-the-start/> (Google “wanted an unrealistic rate of return on basic infrastructure” and lost patience, moving from characterizing its project as “‘experiment’ (2010), then a ‘business’ (2012), and finally a ‘bet’ or ‘moonshot’ (2015)”).

<sup>15</sup> Kansas City Star Editorial, Google Fiber has changed Kansas City but hasn’t Transformed it (Sept. 24, 2017), <https://www.kansascity.com/opinion/editorials/article174936081.html>.

<sup>16</sup> Benjamin Freed, Louisville, Ky. loses Google Fiber after company placed lines too shallow, State Scoop (Feb. 7, 2019), <https://statescoop.com/louisville-ky-loses-google-fiber-after-company-placed-lines-too-shallow/>. Google Fiber later agreed to pay to fix the streets. Jon Porter, Google will pay Louisville millions to fix roads after failed Fiber experiment, The Verge (Apr. 16, 2019), <https://www.theverge.com/2019/4/16/18381466/google-fiber-louisville-kentucky-3-84-million-road-repair-shallow-trenching-service-cancelled>.

company acted in bad faith, but rather that business priorities change and public entities should be leery of leaning too heavily on vendor promises.

When it comes to Quayside, however the public digital governance efforts evolve, the lack of digital governance for the MIDP means that governance will necessarily be post hoc and retrofitted onto MIDP installations. No digital governance regime can ever cover all future contingencies, but in this case, even basic enforceable rules around Quayside data flows are lacking. When Ms. Verner says that “[i]ssues relating to personal data and privacy have not been formally agreed to or implemented at this stage of the Quayside Project,”<sup>17</sup> it is to reassure that problems can be addressed later. For the reasons set forth above, they should be addressed before a plan is adopted. While it is beyond the scope of this opinion to say what those rules should be, among the elements they might include, by way of example, are: A position on what DSAP calls the total “surveillance load” people should be expected to bear;<sup>18</sup> the establishment of no-go zones for data collection (e.g., within the home) or no-go data types (e.g., facial recognition);<sup>19</sup> and steps to protect the public interest when data gathered in Quayside is used to produce new data derivatives (e.g., as AI training data).<sup>20</sup>

#### B. WT’s Review of Project “Solutions” Piecemeal Creates Blind Spots

Scoping the data and privacy challenges is a critical part of addressing them. Sidewalk scopes them narrowly. The MIDP and DIA focus on the data flows associated with the 160 proposed “solutions,” solution-by-solution. By accepting this framing, WT assesses the privacy risks piecemeal, and not holistically. It apparently accepts Sidewalk’s claim “that less than half of the digitally enabled solutions would collect data that may be considered personal information.”<sup>21</sup> In so doing, it reduces the inquiry to a few dozen applications as if they would operate in isolation and not in a data and physical ecosystem where applications are connected to each other and to other urban systems. Consideration of Project proposals individually creates governance blind spots, ignoring the total “surveillance load” that Quayside residents and visitors will experience or how the technologies interact with each other to affect behavior.

So long as privacy assessments start with the proposed technologies, there is no opportunity to consider their necessity or proportionality as compared to other approaches. That Sidewalk says it will practice “digital restraint” is no substitute for a transparent public assessment upfront of the costs and benefits of certain data flows, including how that assessment changes

---

<sup>17</sup> Verner Affidavit at 20.

<sup>18</sup> DSAP Supplemental at 10 (defining surveillance load as the “extent to which individuals’ activities are measured, monitored, or otherwise tracked, regardless of whether the captured information can be associated with an identifiable individual”).

<sup>19</sup> For this and other recommendations, see Keri Grieman, Smart City Privacy in Canada (Jan. 2019), [https://smartcityprivacy.ca/wp-content/uploads/2019/03/Greiman-OPC-Report\\_Final-2019.pdf](https://smartcityprivacy.ca/wp-content/uploads/2019/03/Greiman-OPC-Report_Final-2019.pdf)

<sup>20</sup> Jan Whittington, Remembering the Public in the Race to Become Smart Cities, 85 UMKC L. Rev. 925, 929 (2017) (“Perhaps one of the most important first steps a municipality can take is to begin recognizing that its datasets are, in and of themselves, important assets to be protected in the public interest.”)

<sup>21</sup> WT Round Two Discussion Guide at 10.

if it turns out that data is in fact collected, shared, or otherwise exploited in ways that would be considered unacceptable.

Another kind of blind spot created by WT's piecemeal evaluation is that it doesn't address how the network of technologies Sidewalk proposes will monetize human behavior. Digital information platforms, like Google and Facebook, extract data from online media consumption, social activity, and commerce to better sell people goods and services.<sup>22</sup> While Sidewalk promises not to sell personal data to advertisers, data use by Quayside vendors will shape city services, turning the city into a platform of sorts.<sup>23</sup> We are familiar with special purpose platforms like Uber for transport and Airbnb for accommodations. An intermediary brokers exchanges based on the data it gathers, allowing it to create new markets and commodities. The "city as platform" would deliver all manner of services, including sanitation and public realm access, through a data-mediated exchange with Sidewalk or another vendor in the middle. This model raises concerns about public entity access to data that is collected and managed by private vendors, and more generally about whether the sort of platform-based marketization of services will be in the public interest.<sup>24</sup> Even if particular technologies handle data flows well, the cumulative effect of surveillance-based service provision may modify human behavior, labor, and the provision of goods and services in ways that are unwelcome and will be hard to change once actualized.<sup>25</sup>

Canadian media have reported that Sidewalk at one point produced a "yellow book" outlining at least what at one point were the company's plans for Quayside data: introducing unique identifiers for individuals and organizations in the neighborhood, creating comprehensive data profiles for residents, using a social credit system to reward residents for good behavior with free and premium services, and using data for predictive policing.<sup>26</sup> Whether or not these plans are ever realized, an assessment of any single "solution" or all of them one by one would not reveal the impact of data integration on individuals in Quayside or whether there was consent to such uses.

\*\*\*

---

<sup>22</sup> See NICK SRNICEK, PLATFORM CAPITALISM (2016).

<sup>23</sup> See Kelsey Finch & Omer Tene, Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town, 41 Fordham Urb. L.J. 1581, 1584 (2015).

<sup>24</sup> See SARAH BARNES, PLATFORM URBANISM: NEGOTIATING PLATFORM ECOSYSTEMS IN CONNECTED CITIES (2019).

<sup>25</sup> See generally SRNICEK for the economic and social tendencies of different kinds of digital platforms. Platforms in connection with internet-of-things devices are discussed at 49-53.

<sup>26</sup> Tom Cardoso & Josh O'Kane, Sidewalk Labs Document Reveals Company's Early Vision for Data Collection, Tax Powers, Criminal Justice, The Globe and Mail (Oct. 30, 2019), <https://www.theglobeandmail.com/business/article-sidewalk-labs-document-reveals-companys-early-plans-for-data/>. The response from Sidewalk was that the "Yellow Book" was simply a feasibility study. See Meagan Simpson, Dan Doctoroff Still Believes Sidewalk Labs Can Build a Smart City, Canadian Startup News (Nov. 1, 2019), <https://betakit.com/dan-doctoroff-still-believes-sidewalk-labs-can-build-a-smart-city/>.

WT seems to defer to Sidewalk’s privacy assurances and omnibus promise to comply with later-adopted public digital governance regimes. Agreements between government and private vendors to plan and install digitally-enabled urban infrastructure have long-range consequences, not all of which can be mitigated after the fact even assuming robust enforcement capability. When these agreements are executed before there is a governance structure for data capture and use, the facts on the ground cannot necessarily be changed after that governance takes form. This lag between planning and governance increases the risks to privacy.

## II. Adequacy of Project’s Privacy Protections and Consent Provisions

In the absence of comprehensive and binding public digital governance, privacy protection in Quayside depends heavily on Sidewalk’s promises contained in the MIDP and related documents. Of the MIDP’s 160 proposed “solutions,” 59 are “digitally enabled.” These are technologies that “collect, process, and/or use data about the physical environment around them to improve urban interaction.”<sup>27</sup> These are the focus of WT’s, and commentators’ concerns about privacy and other digital governance issues. Sidewalk promises that it will not sell personal information, not use personal information for advertising, and not share personal information with third parties, including other Alphabet companies, without explicit consent.<sup>28</sup> It also promises to minimize the collection of personal information and to de-identify by default.<sup>29</sup> These promises are not adequate to secure the consent from, and protect the privacy of, people in Quayside.

The following will address these points: A. Sidewalk’s proposed “solutions” will likely collect and use more personal information than is disclosed. B. De-identification of this personal information is not always possible and, in any case, cannot be relied upon as an enduring source of privacy protection. C. Sidewalk overstates the adequacy of notice and consent for the gathering and use of personal information on an “opt-in” basis. D. Assurances about not sharing personal information or sharing only “aggregate information” deflect from the fact that personal information does not have to be shared to be used in privacy-compromising ways. E. The MIDP and related documents do not address the rather significant issue of how Sidewalk will use data collected by other Alphabet companies. I have read and endorse the conclusions that Zeynep Tufekci reaches in her Affidavit about privacy, consent, and security, which overlap with and expand upon the conclusions reached below.

### A. The MIDP Understates the Role of Personal Information

Sidewalk’s privacy scaffolding classifies data into four groups: personal, non-personal, de-identified, and aggregate.<sup>30</sup> Sidewalk claims that no more than 40% of its digitally-enabled

---

<sup>27</sup> WT Round 2 Discussion Guide at 10.

<sup>28</sup> DIA at 43.

<sup>29</sup> DIA at 44.

<sup>30</sup> The MIDP uses Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), to define “personal information,” but its own definitions of the other categories. PIPEDA defines personal information as

subsystems collect personal information,<sup>31</sup> which WT seems to accept.<sup>32</sup> The MIDP may well understate how much personal information will be collected and used.

Among the technologies that collect personal information are the “Energy Home Scheduler,” which would collect unit-level energy usage data;<sup>33</sup> the “Waste Management” system which would collect unit-level waste disposal data to implement a “pay-as-you-throw” regime;<sup>34</sup> and the “Logistics/Freight Management” system, which would collect personal information in order to control package delivery.<sup>35</sup> These applications are predicated on fine-grained data about consumption habits, domestic habits, location information, and other personal data. They are forms of algorithmic regulation, based on personal profiling, which Karen Yeung has defined as “decisionmaking systems that regulate a domain of activity in order to manage risk or alter behavior through continual computational generation of knowledge from data emitted and directly collected (in real time on a continuous basis) from numerous dynamic components pertaining to the regulated environment in order to identify and, if necessary, automatically refine (or prompt refinement of) the system’s operations to attain a prespecified goal.”<sup>36</sup>

These particular algorithmic regulatory systems are likely to be at the core of the Quayside infrastructure, influencing how the built environment is arranged and functions. Once they are in place, it may be difficult to unwind the data flows. Where there is inadequate public governance in place to control what data can be collected and how used, privacy regulation may default to user agreements between the vendor and the people in Quayside. What past digital governance fiascos have demonstrated is that user agreements push users into relinquishing data without clear understanding or recourse, because it is burdensome or impractical to do otherwise.<sup>37</sup> For the Quayside resident to opt-out, or avoid opting-in, to the acquisition of their waste disposal data would require them to have other options. There do not appear to be any plans, either from Sidewalk or WT, for the product and service redundancy necessary to make that optionality real.

---

information about an “identifiable individual.” <https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/159208/sc-2000-c-5.html>. According to Office of the Privacy Commissioner of Canada, “information will be about an ‘identifiable individual’ where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.” [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations\\_02/#fn1-rf](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/#fn1-rf).

<sup>31</sup> DIA at 43 (“60% subsystems do not generate personal information”).

<sup>32</sup> WT Round 2 Discussion Guide at 10 (“Sidewalk Labs stated that less than half of the digitally enabled solutions would collect data that may be considered personal information”).

<sup>33</sup> MIDP, Volume 2 at 316.

<sup>34</sup> MIDP, Volume 2 at 350.

<sup>35</sup> MIDP, Volume 2 at 352.

<sup>36</sup> Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Regulation & Governance 505 (2018).

<sup>37</sup> See generally, K.B. Cornelius, Zombie contracts, dark patterns of design, and ‘documentisation,’ Internet Policy Review, 8(2) (2019), <https://policyreview.info/node/1412/pdf>.

For other proposed technologies, where Sidewalk claims that no identifiable personal information is required, it is difficult to understand how these would work without personal data. For example, the “Outcome-Based Code” proposes to use sensors to monitor compliance with nuisance-standards for building use – things like noise levels or odor discharges.<sup>38</sup> An outcome-based code for property use is a way to allow uses formerly classed as incompatible to co-exist, subject to limits on the harms property users may permissibly impose on their neighbors. Personal information is what makes the code enforceable. WT does not challenge Sidewalk’s assertion that the code would not collect personal information. Nor does it address how code limits can be enforced without tracing harm (noise, smell, vibration) to the individual responsible. For another solution – Efficient Building Lighting – Sidewalk acknowledges that personal information *would be* needed. This would be tenant-level lighting and occupancy data in order to optimize energy use.<sup>39</sup> For HVAC-Performance Monitoring, which is part of Sidewalk’s sustainability package, thermal energy use would be collected.<sup>40</sup> But here, Sidewalk says that the humidity data gathered would be either non-personal or de-identified. If the purpose of energy use reporting is to reward and encourage sustainable practices, it would seem the data would have to be associated with a personal account. If there are novel technologies to mask identity in this system, they are not made transparent and subject to public accountability.

## B. Over-Reliance on De-Identification

Many of the Project’s proposed “solutions” downplay the privacy implications of data flows by promising to “de-identify” data. According to Sidewalk, “de-identified data is data about an individual that was identifiable when collected but has subsequently been made non-identifiable.”<sup>41</sup> Dr. Tufekci critiques data de-identification as one of the Project’s main privacy-protection strategies.<sup>42</sup> There is a scholarly consensus that de-identified or anonymized data can be re-identified or de-anonymized relatively easily, so that nearly any piece of information collected from and about an individual should be deemed personal data.<sup>43</sup> With respect to the Project in particular, the DSAP Supplemental Report finds that “Sidewalk overly relies on de-identification at source as a sufficient basis for making personal data open for re-use.”<sup>44</sup> And Canadian legal scholar Lisa M. Austin, whom Sidewalk cites favorably in connection with her

---

<sup>38</sup> DIA at 82-84.

<sup>39</sup> DIA at 91.

<sup>40</sup> DIA at 89

<sup>41</sup> DIA at 49.

<sup>42</sup> The Affidavit of Zeynep Tufekci, sworn June 4, 2019, at 5-7 (“Tufekci Affidavit”).

<sup>43</sup> See generally Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010) (critiquing inadequacy of de-identification techniques). See also Lisa M. Austin, Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices, 44 Can. Bus. L.J. 21, 35-36 (2006) (discussing the consequences of re-identification under Canada’s PIPEDA); Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. REV. 1814, 1836-48 (2011) (discussing re-identification of Google, AOL, and Netflix users).

<sup>44</sup> DSAP Supplemental p 14.

ideas about data sharing, argues that Sidewalk’s de-identification approach to sharing information “is a flawed strategy.”<sup>45</sup>

Some examples of Sidewalk’s proposals illustrate the problems. Sidewalk reports that the “dynamic curb” will use de-identified information to assess use of the public realm. If that data is re-identified, it would be possible to derive personal location information about people moving about Quayside.<sup>46</sup> Dr. Tufekci notes in connection with location data:

The kind of data that Sidewalk Labs is considering collecting almost certainly could be useful for much deeper computational inference than the surface aspects of the data. For example, in my opinion, regular location data can almost certainly be used to predict many health considerations, including mental health status, or private information.<sup>47</sup>

Sidewalk asserts that its Mobility-as-a-Service solution will rely on de-identified data that gives third-party users the ability to “check the user’s remaining balance” of rides.<sup>48</sup> De-identified mobility data is proving to be highly controversial. In Los Angeles for example, where the city is requiring ride-sharing companies like Lime and Uber to share de-identified ride information, there has been significant push back on the privacy implications.<sup>49</sup> Studies have shown that this kind of data is easily re-identified.<sup>50</sup>

Other Project proposals raise the question not only of whether de-identification is a persistent feature, but also whether it can be a feature at all in light of the solution’s goals. As noted above, building code monitoring to determine whether noise exceeds permitted levels is said to rely on de-identified noise level information. It is hard to imagine nuisance enforcement against individuals for excessive noise if that data is de-identified.<sup>51</sup>

There are too many examples of technology companies promising to anonymize personal information, but then compromising that anonymity, to rely on assurances of de-identification.<sup>52</sup> For example, Apple has reportedly shared “anonymized” Siri-recorded highly personal conversations with contractors even though such use is not disclosed in the Apple user agreement. These recordings are accompanied by user data showing location, contact details,

---

<sup>45</sup> Lisa M. Austin & David Lie, *Safe Sharing Sites*, 94 N.Y.U. L. Rev. 581, 590–91 (2019) (pointing out that strategies to minimize the risks of re-identification compromise the accuracy of the data).

<sup>46</sup> DIA at 62.

<sup>47</sup> Tufekci Affidavit at 14.

<sup>48</sup> DIA at 67.

<sup>49</sup> Andrew J. Hawkins, *Uber threatens to sue Los Angeles, as the fight over scooter data escalates*, The Verge, <https://www.theverge.com/2019/10/29/20938212/uber-lawsuit-la-ladot-scooter-data-mds> (Oct 29, 2019).

<sup>50</sup> Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, *Scientific Reports* 3, no. 1 (March 25, 2013): 1376, <https://doi.org/10.1038/srep01376>.

<sup>51</sup> DIA at 84.

<sup>52</sup> See, e.g., Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* at 22-24 (2019), <https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF>.

and app data.<sup>53</sup> Amazon has had Alexa-captured conversations transcribed in order to further research and development<sup>54</sup> and YouTube, a Google company, was fined \$170 million by the U.S. Federal Trade Commission in 2019 for mining the anonymized data of children.<sup>55</sup> In its announced collaboration with Apple to build coronavirus contact-tracing technology, Google itself tacitly acknowledges the privacy advantages of never collecting personal information in the first place over scrubbing identifiers out. The companies' proposed technology therefore requires no personal information in order to trace the potential transmission of the virus.<sup>56</sup>

### C. Inadequacy of Notice and Consent for Personal Information Collection

Some of the Project's proposed "digitally-enabled solutions" that do rely on personal information purport to be opt-in and subject to notice and consent. The adequacy of the notice and meaningfulness of consent are both problems. Legal scholars Neil Richards and Woodrow Hartzog identify the dangers of "unwitting consent" and "coerced consent" in digital contexts. Consent is insufficiently "knowing" when the user does not understand the technology being agreed to or the practical consequences of agreeing. Consent is insufficiently "free" when a person must choose between consent and the loss of an important function or asset.<sup>57</sup> The Project poses both of these dangers to a significant degree.

One example of the Project's opt-in notice and consent regime in operation is the "Dynamic Curb."<sup>58</sup> The proposal is for individuals to opt-in to locate parking and provide parking payment. This kind of opt-in is only meaningful if there are alternative payment methods and modes of access. As an analogy, electronic toll collection on highways is not really optional if there is no other way to pay for use of the road. The toll collector has a monopoly on that road and, therefore, on the means of collection. Nowhere in the MIDP could I find a plan for how people who choose *not* to opt-in can still access Quayside's infrastructure.<sup>59</sup> The "Enhanced Electric Vehicle Charging" and "Mobility as a Service"<sup>60</sup> proposals pose the same problems. The first

---

<sup>53</sup> Alex Hern, Apple contractors 'regularly hear confidential details' on Siri recordings, *The Guardian*, <https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings>, (July 27, 2019), <https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-onsiri-recording>.

<sup>54</sup> Ry Crist, Amazon and Google are listening to your voice recordings. Here's what we know about it, *CNET* (July 13, 2019), <https://www.cnet.com/how-to/amazon-and-google-are-listening-to-your-voice-recordings-heres-what-we-know/>.

<sup>55</sup> Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 *Wash. U.L. Rev.* 1461, 1466 (2019).

<sup>56</sup> Apple & Google, *Privacy-safe contact tracing using Bluetooth Low Energy*, [https://blog.google/documents/57/Overview\\_of\\_COVID-19\\_Contact\\_Tracing\\_Using\\_BLE.pdf](https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf). The system will create and verify a user's identity with a secret "tracing key," which is created and stored on a user's device rather than ever going to a company or government authority. The tracing key is then used to generate information that is used to trace contact.

<sup>57</sup> See Richards & Hartzog.

<sup>58</sup> MIDP, Volume 2 at 451.

<sup>59</sup> In his interview with the BBC World Service, Sidewalk executive Rit Aggarwala suggested that opt-out could be achieved by choosing not to live in or visit Quayside. See Aggarwala interview ("Nobody is ever going to be forced to live in or visit this neighborhood").

<sup>60</sup> DIA at 66-69.



would provide an opt-in subscription service for vehicle charging. The second would allow users to opt-in subscription for car and other vehicle-shares. Again, opt-in is meaningful only if there are adequate alternatives for those who would choose not to.

On top of the difficulty of truly free consent is the problem of meaningful notice. To be meaningful, notice should make users understand how their location and other personal data are being used. We do not know much yet about how notice will be effectuated for people in Quayside. The MIDP and DIA suggest that for some technologies, notice about what data is collected and how it will be used will be in user agreements. For example, this is the case with the public Wi-Fi.<sup>61</sup> As discussed in Part III, people have not been able to rely on user agreements as a source of meaningful notice because the companies have flouted or changed them after users are effectively captive to the service.

Sidewalk has proposed another method of providing notice in cases where user agreements are not practical: physical signage showing people in Quayside what kinds of data may be collected.<sup>62</sup> Such signage provides some notice, but does not inform people how their data will be used. As Dr. Tufekci writes, “It may not be possible to give informed consent to data collection of this scale because the data can reveal a lot more than one imagined, thus making it difficult for an ordinary person to be meaningfully informed.”<sup>63</sup> Moreover, consent to the data collection cannot be inferred from mere acquiescence if people do not have practical alternatives. If, for example, personal information is collected by all sanitation services, it would be unreasonable to expect people to decline the service (even if that were legal) as a means of withholding consent. Even if there are non-surveillant alternatives, it is sometimes too costly to refrain from consenting. Privacy can “unravel” when most people are willing to disclose their personal information, casting suspicion, stigma, or even penalty on those who refuse.<sup>64</sup> The MIDP and other Project documents do not address these limits of the Project’s proposed notice and consent structures.

Finally, security lapses vitiating consent to data collection and use. Sidewalk proposes to use an application programming interface (API) – a portal that connects third parties to data – to provide government and private parties with access to Quayside-related data. As Dr. Tufekci points out, Google’s APIs have proven vulnerable in the past to unauthorized access. The company closed its social media network Google+ after discovering “that a bug had exposed the data of more than half a million Google+ users for about three years.”<sup>65</sup> An internal investigation showed that 100,000 private user data points had been leaked. This kind of hack

---

<sup>61</sup> DIA at 74.

<sup>62</sup> DIA at 55.

<sup>63</sup> Tufekci Affidavit at 15 (using the example of Strava fitness application data used to reveal American military personnel movements).

<sup>64</sup> Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 *Nw. U. L. Rev.* 1153, 1156 (2011).

<sup>65</sup> Tufekci Affidavit at 10.

and other security concerns discussed in her Affidavit show the vulnerability of data-intensive applications to security breaches.

Here, it is worth mentioning two technologies that Sidewalk advances to safeguard personal data: Distributed Verifiable Credentials (DVC)<sup>66</sup> (encrypted code that resides on personal devices and can be used for identification purposes, in lieu of sharing personal information) and a Software Defined Network<sup>67</sup> (a wireless “home” network and data storage that travels with people so they can avoid accessing third-party networks and cloud storage). These may be promising technologies, but whether they increase security and secure privacy, or simply create new vulnerabilities and exposure, will depend on governance. Sidewalk suggests that people could use DVC to submit housing applications, gain access to the dynamic curb, and submit energy consumption data.<sup>68</sup> If DVC are not adopted, or not adopted in a privacy-protective fashion, then these key parts of Quayside operations may require more personal information than the MIDP suggests. Everything about DVC – how the technology would function and be governed – is tentative and contingent. It is unclear what services will depend on the technology and how people might opt out. At the same time, the technology seems to undergird essential digital architecture. As with many aspects of the Project, it is left vague what Alphabet companies’ roles will be in owning<sup>69</sup> and establishing the rules for DVC and Software Defined Networks, and what the digital governance costs might be.

#### D. Data Derivatives

Taking Sidewalk at its word that it will not share personal data with third parties or other Alphabet companies without consent, there are privacy risks even where personal information is not shared in raw form. Personal data may be used to train algorithms or derive inferences about people, which inferences are then sold or otherwise shared. Facebook is perhaps best-known for this practice, creating “lookalike audiences” for advertisers who want users that look like their existing customers.<sup>70</sup> Facebook has also reportedly been able to infer sexual orientation and depression from personal information, which inferences it sells even if it does not share the personal information itself.<sup>71</sup> Data from smart home devices or from smart wearables, like hearing aids, can be processed as an input into other products that build on

---

<sup>66</sup> DIA at 170-182.

<sup>67</sup> DIA at 147-156.

<sup>68</sup> DIA at 173-4.

<sup>69</sup> Sidewalk states that it “would not build this technology.” DIA at 175.

<sup>70</sup> See Giridhari Venkatadri, et al., Privacy Risks with Facebooks PII-Based Targeting: Auditing a Data Brokers Advertising Interface, 2018 IEEE Symposium on Security and Privacy (SP) (2018), [https://www.ftc.gov/system/files/documents/public\\_events/1223263/p155407privacyconmislove\\_1.pdf](https://www.ftc.gov/system/files/documents/public_events/1223263/p155407privacyconmislove_1.pdf).

<sup>71</sup> See Sandra Wachter & Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, 2019 Colum. Bus. L. Rev. 494, 506–08 (2019); Michal Kosinski, David Stillwell & Thore Graepel, Private Traits and Attributes Are Predictable from Digital Records of Human Behavior, 110 Proc. Nat’l Acad. Sci. 5802 (2013).

these data derivatives.<sup>72</sup> In all these cases, companies are monetizing data without sharing or selling personal information. The creation of these unforeseen products was not and could not be consented to.

Google does not need to share the search and YouTube history it collects by default in order to use that data to shape what a person learns and sees. In the same vein, Sidewalk does not need to share personal information in order to exploit derivatives of that data. The Project's physical and social infrastructure – housing, offices, public space, transit, health care, education, sanitation, energy – will be built around a “digital layer” of data flows.<sup>73</sup> The data will presumably inform government and other entities about personal energy consumption, location, rubbish disposal, and transit. Sidewalk and other companies can use the information to create profiles. These in turn can be used (and sold) as inputs into algorithmic risk assessments, pricing, or advertising, or to otherwise shape people's experiences and opportunities. These are uses to which people cannot meaningfully consent. As Dr. Tufekci notes, “It's quite difficult for ordinary people to be informed about all such uses of their data because new computational algorithms can take seemingly irrelevant data and produce insights in all sorts of domains.”<sup>74</sup> Knowing what an algorithm will do with data is unknown not only to the user, but to the domain experts themselves as algorithms behave in unexpected and unexplainable ways.<sup>75</sup>

Another possible derivative product of personal information is “aggregate data” – the MIDP category that is treated as separate from personal information. Sidewalk denotes “aggregate data” as “data that is about people in the aggregate and not about a particular individual,” suggesting that this class of data poses minimal privacy concerns. Even if aggregate data cannot be disaggregated – a disputed point – that does not end the inquiry. There is still the question of whether the compilation and use of aggregate data increases the collection of personal information in the first place. If aggregate data uses personal data as an input, it is a personal data derivative. Derivatives of all kinds, if valuable, will likely encourage the collection of personal data and thereby increase the total surveillance load.

One of Sidewalk's proposed technologies would “aggregate counts of people in an office space” with other data to control energy usage. Such aggregate data might simply count human bodies or it might use personal location data. In both cases, it is aggregate data, but the kind of data input makes a meaningful difference to how much personal data is collected and exploited.

---

<sup>72</sup> See, e.g., Kennedy, Krista and Wilson, Noah and Tschider, Charlotte, *Balancing the Halo: Data Surveillance and Algorithmic Opacity in Smart Hearing Aids* (January 11, 2020) at 21 (“What might begin as collecting data on the sound levels deaf wearers prefer for conversations in order to better calibrate devices, might easily be re-processed as marketing research data on wearers that can then be sold ... to other entities for commercial benefit.”), available at <https://ssrn.com/abstract=3521614> or <http://dx.doi.org/10.2139/ssrn.3521614>

<sup>73</sup> DIA at 51.

<sup>74</sup> Tufekci Affidavit at 15.

<sup>75</sup> See, e.g., Jenna Burrell, *How the Machine “Thinks”: Understanding Opacity in Machine Learning Algorithms*, *BIG DATA & SOC'Y*, Jan.–June 2016, at 1, 3–5.

Citing to this definitional sloppiness, one DSAP Commenter writes that “further use of these [MIDP] categories is not reliable.”<sup>76</sup> At the very least, neither the classification of information as “non-personal” nor the assurances that vendors will not share personal data suffice to ensure privacy protection.

### E. The Negative Space of Digital Governance

Outside the four corners of what Sidewalk says about data flows, there are omissions that may be just as significant. For example, unaddressed is the question of how the proposed “solutions” will incorporate third-party information about the people in Quayside, whether that be credit-card information, health information, or Google search and Android data. Sidewalk has said it will not share personal information, including with other Alphabet companies, without explicit consent.<sup>77</sup> This statement says nothing about whether Sidewalk will use data that other companies – especially Alphabet companies -- have collected.

Google collects data via tracking built into the Chrome browser and Android operating system, through websites that use Google Analytics, through its ubiquitous ad-serving software AdSense, from Google search and many other touch points. When Alphabet CEO Sundar Pichai appeared before the U.S. Congress’ Judiciary Committee, he did not deny Chairman Goodlatte’s observation that Android alone “sends Google information every few minutes, detailing the exact location of a smart phone within a few feet, the speed of movement of the phone, the altitude of the phone, sufficient to determine what floor of a building the phone is on, the temperature surrounding the phone ... [meaning] that Google is compiling information about virtually every movement an individual with a smart phone is making, every hour of every day.”<sup>78</sup> If we add to this what Google knows from its Maps, Gmail, Home, and other products existing and forthcoming, Google holds a lot of data about individuals. I could not find in the documents a statement by Sidewalk about how this data will or will not be integrated into Quayside applications.

### III. Past Practice of Alphabet/Google and other Technology Companies

University of Toronto professor emeritus Andrew Clement, who is a member of the DSAP, notes that Sidewalk’s “statements are not always consistent and [are] at times contradictory,” raising concerns about how its plans “can be treated as reliable evidence of its actual intentions.”<sup>79</sup> The history of Alphabet subsidiary companies, and of other technology companies, counsels caution about the longevity and enforceability of promises. These companies have often failed to live

---

<sup>76</sup> DSAP Supplemental at 51.

<sup>77</sup> DIA at 257.

<sup>78</sup> U.S. House Judiciary Committee Hearing on Transparency and Accountability: Examining Google and Its Data Collection, Use and Filtering Practices, Dec. 11, 2018.

<sup>79</sup> Josh O’Kane, Waterfront Toronto’s digital panel says it is not confident all of Sidewalk Labs’s data collection would be justified, *The Globe & Mail* (Feb. 26, 2020), <https://www.theglobeandmail.com/business/article-waterfront-torontos-digital-panel-says-it-is-not-confident-all-of/>.

up to their own digital governance commitments and enforcement mechanisms have been weak.

The following provides examples of companies – in most cases, Alphabet subsidiaries -- backtracking on digital governance promises made to end-users and/or to public bodies. What these examples show is an inexorable tendency to collect and exploit data more intensively than the original technology deployments suggested they would, with the resulting expansion of the surveillance load. Where this expansion contravenes the initially agreed terms of service, and where opt-out is not practicable, the additional surveillance is in no way legitimized by user consent.

#### A. Misleading or Broken Data Sharing Promises: Alphabet DeepMind.

Sidewalk promises that it will not, without user consent, share personal information collected in Quayside, even with other Alphabet companies.<sup>80</sup> The London-based health AI firm, DeepMind – an Alphabet subsidiary – made the same promises in connection with a partnership with the UK’s National Institute of Health. Privacy advocates were concerned that DeepMind would link the public’s personal health data with Google data. This concern intensified when DeepMind was integrated into the parent company.<sup>81</sup> While DeepMind continues to assert that use of the patient data is at all times subject to the control of the health care providers, in actuality, there is no way to know this or audit it. This issue arose after an earlier dustup in which the UK Information Commissioner’s office found that the Royal Free National Health Service Foundation Trust had illegally shared sensitive patient data with DeepMind without adequate consent.<sup>82</sup>

#### B. Misleading or Broken Data Collection Promises: Android, Google Education, YouTube

Sidewalk promises that users will be informed about when embedded technologies are collecting personal information and be able to exercise control. Google has made similar promises in connection with the use of Android phones. Associated Press reporters discovered in 2018 that Android phones continue to collect location information even after users had disabled “Location History,”<sup>83</sup> which is all that Google’s user guide seemed to require. Google

---

<sup>80</sup> DIA at 226 (Sidewalk “also commits to not share personal information with third parties, including other Alphabet companies, without explicit consent.”).

<sup>81</sup> See Alex Hern, Google ‘Betrays Patient Trust’ with DeepMind Health Move, *Guardian* (Nov. 14, 2018), <https://www.theguardian.com/technology/2018/nov/14/google-betrays-patient-trust-deepmind-healthcare-move> (reporting that the DeepMind app’s cofounder stated that “at no stage [would] patient data ever be linked or associated with Google accounts, products or services”).

<sup>82</sup> See also Cara McGoogan, NHS Illegally Handed Google Firm 1.6m Patient Records, UK Data Watchdog Finds, *Telegraph* (July 3, 2017), <https://www.telegraph.co.uk/technology/2017/07/03/googles-deepmind-nhs-misused-patient-data-trial-watchdog-says> (reporting on finding that DeepMind and the NHS violated the UK’s Data Protection Act of 2017 by failing to provide enough transparency or data protections); Julia Powles & Hal Hodson, Google DeepMind and healthcare in an age of algorithms, 7 *Health Technologies* 351 (2017) (detailing how DeepMind violated privacy laws and prior promises).

<sup>83</sup> Ryan Nakashima, Google tracks your movements, like it or not, *Associated Press* (Aug. 13, 2018), <https://apnews.com/828aefab64d4411bac257a07c1af0ecb>.

subsequently revised its user guide to tell users that they would have to also turn off “Web and App Activity” -- another function that is enabled by default. Australia’s competition watchdog has now sued Google over the issue, claiming that Google misled consumers about the collection and use of location data.<sup>84</sup>

Google Education has also made misleading promises regarding students’ privacy rights. According to investigations, Google was mining students’ browsing data and other information, despite publicly promising not to so.<sup>85</sup> As a result, New Mexico has recently sued Google for breaking its privacy promises. It alleges that Google “has been making public statements and promises that are designed to convince parents, teachers, and school officials that Google takes student privacy seriously and that it only collects education-related data from students using its platform. Google has also publicly promised never to mine student data for its own commercial purposes.” It goes on to allege that “Google has broken those promises... by collecting troves of ... personal information” including students’ physical locations, visited websites, search terms, identities of YouTube videos watched, personal contact lists, voice recordings, saved passwords, and other behavioral information.”<sup>86</sup>

In another legal action, Google paid a financial settlement in response to a complaint by the US Federal Trade Commission and New York Attorney General alleging that YouTube violated the Children’s Online Privacy Protection Act by collecting personal information from viewers of child-directed channels without parental consent. YouTube then used the data to deliver targeted ads to viewers of these channels.<sup>87</sup>

### C. Terms of Service Changes and Meaningless Consent: Google Nest

Like DeepMind, the smart home product Nest (a subsidiary of Google LLC) promised that the data it collected would remain separate from users’ Google profiles. People installed Nest products in their homes presumably relying on this promise. In May 2019, Google decided to integrate Nest into its smart home suite of products. Nest then changed its terms of service, stating that the Nest data would be combined with the rest of Google’s data.<sup>88</sup> One of the possibilities is that users’ commands given in their home and perhaps even the facial

---

<sup>84</sup> Australian Competition and Consumer Commission, Google allegedly misled consumers on collection and use of location data, 29 Oct. 2019, <https://www.accc.gov.au/media-release/google-allegedly-misled-consumers-on-collection-and-use-of-location-data>.

<sup>85</sup> Electronic Frontier Foundation, [https://www.eff.org/wp/school-issued-devices-and-student-privacy#footnoteref24\\_1pimoal](https://www.eff.org/wp/school-issued-devices-and-student-privacy#footnoteref24_1pimoal) (citing, Google response to Sen. Al Franken. (Feb. 12, 2016). <https://www.franken.senate.gov/files/letter/160216GoogleResponse.pdf>)

<sup>86</sup> State of New Mexico v. Google LLC, Complaint, District of New Mexico (Feb. 20, 2020), [https://cdn.vox-cdn.com/uploads/chorus\\_asset/file/19734145/document\\_50\\_.pdf](https://cdn.vox-cdn.com/uploads/chorus_asset/file/19734145/document_50_.pdf).

<sup>87</sup> FTC, Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law (Sept. 4, 2019), <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>

<sup>88</sup> Jessica Baron, Google’s New Nest Hub Max Raises Questions About How Much We Still Value Our Privacy, Forbes (Sept. 9, 2019), <https://www.forbes.com/sites/jessicabaron/2019/09/09/googles-new-nest-hub-max-raises-questions-about-how-much-we-still-value-our-privacy/#428a59af146b>.

recognition properties of the Nest service would be integrated into Google search data and, among other things, used for behavioral advertising.

This example is in keeping with many in which tech companies change their terms of service to rescind data sharing promises. In theory, once consumers are notified of the new arrangement, they can choose to withdraw or grant their consent. In fact, the switching costs and/or network effects attending many technologies make withdrawal difficult.<sup>89</sup> Withdrawal of consent may be even more difficult when it comes to an installed base of internet of things products. People cannot be expected to rip out smart home products like Nest every time a company withdraws privacy protections. This inertia or path dependency works to the benefit of companies that have the autonomy to change course, while depriving individuals of effective autonomy to consent.

#### D. Surveillance Creep: Google Nest

Installing technology in a city without clear digital governance poses a credible threat of “surveillance creep”, i.e., that a technology designed or procured for one thing comes to be used for other purposes.<sup>90</sup> This is not to call out any single Sidewalk proposed solution, but to caution that a vendor-led project planning for a thick weave of special-purpose sensors may deploy that surveillance capability in new ways, without authorization. Google has done this in the past. It took the public by surprise in 2019 when it was revealed that the Google Nest security product had a built-in microphone. As Dr. Tufekci notes, the microphone posed a security risk as well.<sup>91</sup> That capability was not consistent with the function people thought they were getting. Google later admitted that it should have disclosed the microphone which had been built in for future use and was not meant to be secret.<sup>92</sup>

This tendency for devices to expand their capabilities in the future is common in smart-city technologies. Sometimes the creep is from within government deployments. The acoustic gunshot detector used in hundreds of cities (most often the market leader ShotSpotter), for example, also incidentally records human voices. These recordings have controversially been used as evidence in criminal cases.<sup>93</sup> In San Diego, the city council entered into a \$30 million contract with a General Electric company in 2017 to build 4000 smart streetlights in the city.

---

<sup>89</sup> See JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE (2014).

<sup>90</sup> See BRETT FRISCHMANN & EVAN SELINGER, RE-ENGINEERING HUMANITY 20 (2018) (italics in original) (“[s]urveillance creep is an offshoot of what engineers call *function creep*, the idea that a tool designed for one purpose ends up being used for another one”).

<sup>91</sup> Tufekci Affidavit at 11.

<sup>92</sup> Jon Porter, Google claims built-in Nest mic was ‘never intended to be a secret’, The Verge, Feb 20, 2019, <https://www.theverge.com/circuitbreaker/2019/2/20/18232960/google-nest-secure-microphone-google-assistant-built-in-security-privacy>.

<sup>93</sup> Electronic Frontier Foundation, Gunshot Detection, <https://www EFF.org/pages/gunshot-detection>.

The contract alluded to various types of data analytics that the company might provide, including transit and parking information.<sup>94</sup> But it did not surface, nor was council ever alerted to the fact, that the streetlights would have video surveillance capabilities.<sup>95</sup> What was billed as a way to make lights more energy efficient ended up being a trove of data analytics for GE.

Sometimes the creep is from private installations out to the government. For example, the Amazon Ring doorbells which consumers intended to provide surveillance of their homes also came to be used by police departments across the U.S. for neighborhood surveillance.<sup>96</sup>

#### E. De-Identification Bromides: Replica and Intersection

Replica, an Alphabet spin-off, creates what are known as “digital twins” for transportation planning purposes. A twin is a simulation of actual transportation patterns based on supposedly de-identified personal data. It is being used in Kansas City and is under contract in Illinois. Portland Oregon decided not to proceed with a Replica project because, reportedly, Replica did not give the city sufficient information about privacy protections. Replica said that telecoms and credit card companies were among the sources for its data. Portland was not satisfied with how well this personal location data was de-identified. Because data sellers often shroud details of their practices in nondisclosure agreements, it is hard for outsiders to ascertain the origins of the data and the adequacy of privacy-protecting procedures. Portland decided that it could not use Replica without being able to test the efficacy of the de-identification efforts.<sup>97</sup> This is a cautionary story about reliance on a company’s claims of de-identification, especially when that company is not itself the source of the data it is using.

The roll out of LinkNYC WiFi kiosks in New York City also illustrates how de-identification is not a privacy fix. Even more, it shows how public resistance may be needed to rein in a smart city vendor from pursuing maximalist data collection opportunities. In 2016, New York contracted with a private consortium to install a citywide network of 10,000 WiFi hotspots in place of payphones. The consortium leader is Intersection, the digital advertising company, in which Sidewalk is a major investor. The New York Civil Liberties Union complained about how much personal information the consortium planned for the LinkNYC kiosks to collect, including search

---

<sup>94</sup> Intelligent Cities Project, San Diego (Oct. 28, 2016)(contract with General Electric) [https://drive.google.com/file/d/1O09OLau09zsC8nnpk\\_fFgowbdxTo7iG2/view](https://drive.google.com/file/d/1O09OLau09zsC8nnpk_fFgowbdxTo7iG2/view)

<sup>95</sup> Katy Grimes, City of San Diego Awarded GE Mass Surveillance Contract Without Oversight: San Diego is now home to the largest mass surveillance operation across the country, California Globe (Jan. 13, 2020), <https://californiaglobe.com/section-2/city-of-san-diego-awarded-ge-mass-surveillance-contract-without-oversight/>.

<sup>96</sup> Drew Harwell, Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns, Wash. Post (Aug. 28, 2019), <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/?arc404=true>.

<sup>97</sup> Kate Kaye, This Startup Wants to Help Smart cities. But they don’t know where its data comes from, Fast Company (Mar. 6, 2020), <https://www.fastcompany.com/90465315/this-startup-wants-to-help-smart-cities-but-they-still-dont-know-where-its-data-comes-from>.



information and browser history.<sup>98</sup> In response to the publicity and threatened litigation, the city renegotiated the contract. It appears still to be the case, however, that the consortium can capture metadata about any mobile device, even those not connected to the network.<sup>99</sup> This includes information about the type of device, the MAC address (an encrypted version of the device's identification number for WiFi networks), the IP address, the browser and browser plug-ins, and the operating system. While Intersection designates all this information as "technical" rather than "personal," the data can apparently be used to identify when someone is a returning retail customer, a sports event attendee, or commonly with another person based on their proximate devices.<sup>100</sup> Intersection has not disclosed what it plans to do with this data.<sup>101</sup>

Intersection's privacy policy states that users who provided an email address will be notified if the privacy policy changes and will then have an opportunity to stop using LinkNYC "if they do not consent to the changes."<sup>102</sup> As discussed above, for those who rely on LinkNYC for wireless access, this kind of consent may be illusory. As consideration for placing its street furniture in the public right of way, LinkNYC agreed to pay the city a portion of advertising revenue collected from the 9-foot high structures.<sup>103</sup> LinkNYC is now reportedly "delinquent" in the payments in the amount of millions of dollars, and has also reneged on its commitment to build out the kiosks, especially in low-income areas.<sup>104</sup> There has not yet arisen a contract dispute related to data practices, but the difficult the city has had in obtaining the benefit of its bargain in other areas does not bode well for the compliance-through-contract leverage strategy.

\* \* \*

There is insufficient digital governance to ensure that the Project will adequately protect the privacy of and secure the consent of the people of Quayside, especially in light of the recent history of technology company lapses in regard to these goals.

---

<sup>98</sup> New York Civil Liberties Union, City's Public Wi-Fi Raises Privacy Concerns, March 16, 2016, <http://www.nyclu.org/news/citys-public-wi-fi-raises-privacy-concerns>.

<sup>99</sup> BEN GREEN, THE SMART ENOUGH CITY: PUTTING TECHNOLOGY IN ITS PLACE TO RECLAIM OUR URBAN FUTURE 92-95 (2019).

<sup>100</sup> Aaron Shapiro, The true cost of free LinkPHL WiFi might be privacy, The Philadelphia Inquirer (Jan. 9, 2019), <https://www.inquirer.com/opinion/commentary/link-phl-wifi-kiosks-data-privacy-20190109.html>.

<sup>101</sup> Ava Kofman, Are New York's Free LinkNYC Internet Kiosks Tracking Your Movements?, The Intercept (Sept. 8, 2019), <https://theintercept.com/2018/09/08/linknyc-free-wifi-kiosks/>.

<sup>102</sup> March 2017 LinkNYC Privacy Policy, Exhibit 2, CityBridge Privacy Policy, Franchise Agreement for the Installation, Operation, and Maintenance of Public Communications Structures in the Boroughs of the Bronx, Brooklyn, Manhattan, Queens and Staten Island 2 (Mar. 17, 2017), <http://www1.nyc.gov/assets/doitt/downloads/pdf/Proposed-PCS-Franchise-Exhibit-2-CityBridge-Privacy-Policy.pdf>.

<sup>103</sup> Eric Hornbeck, "We Know Not Where We Go": Protecting Digital Privacy in New York City's Municipal Wi-Fi Network, 45 Fordham Urb. L.J. 699, 716-17 (2018).

<sup>104</sup> Dana Rubinstein and Joe Anuta, City Hall Calls Google-backed LinkNYC Consortium 'delinquent', The Politico (03/03/2020), <https://www.politico.com/states/new-york/albany/story/2020/03/03/city-hall-calls-google-backed-linknyc-consortium-delinquent-1264966>.

**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

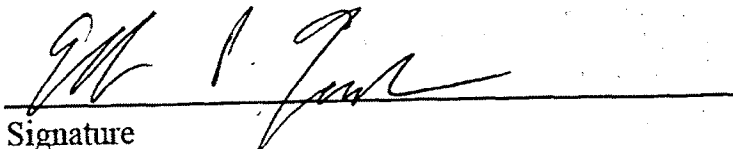
APPLICATION under sections 2 and 6(1) and 6(2) of the *Judicial Review Procedure Act*, R.S.O. 1990, c. J.1, as amended, and sections 2, 7, 8 and 24 of the *Charter of Rights and Freedoms*.

**ACKNOWLEDGMENT OF EXPERT'S DUTY**

1. My name is Ellen P. Goodman. I live in of the City of Philadelphia, in the State of Pennsylvania.
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.

Date: April 29, 2020

Signature



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  
ELLEN P. GOODMAN**

**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

**ELLEN P. GOODMAN**

Rutgers Law School  
 217 N. Fifth Street, Camden, N.J. 08102  
[ellgood@rutgers.edu](mailto:ellgood@rutgers.edu) ~ 856-225-6393 (t); 610-324-9710 (m)

**EDUCATION**

**Harvard Law School**, J.D. *cum laude*. Pew Fellow in International Law 1992  
**Harvard College**, A.B. *magna cum laude*. Harvard Crimson, Philips Brooks House 1988

**EMPLOYMENT**

**Rutgers Law School**. Camden, NJ Professor 2007-present  
 Associate Professor 2003-2007

- *Co-Director*, Rutgers Institute for Information Policy & Law (RIIPL); *Director*, News Law Project: design curricula, programming, student supervision, community outreach
- *Senior Fellow*, German Marshall Fund Digital Innovation & Democracy Initiative
- *Grant Awards (Principal Investigator)*: Knight Foundation (2020-22), Democracy Fund (2019-21), Pratt Award (2016-19), Dodge Foundation (2015-16), Ford Foundation (2010-14). *Current Grant Projects*: Platform regulation; Algorithmic transparency; Reporting project on public algorithms
- *Courses*: digital privacy, global free expression, intellectual property, copyright, media, public media, advertising, property, animal law
- *Scholarly focus*: information law and policy, free expression, public media, transparency policy, data governance and smart cities
- *Policy advisor/speaker*: FCC, U.S. Congress, Natl. Academy of Arts and Sciences, Natl. Academies of Science and Tech., Brookings Institution, Aspen Institute
- *Publish in Slate, Guardian, Protego Press, [medium.com/@ellgood](https://medium.com/@ellgood)*
- *Select Service*: Pittsburgh Task Force on Public Algorithms; Council Member, Civil Media Foundation (blockchain media platform)

**Select Secondary and Visiting Appointments:**

*London School of Economics Senior Visiting Fellow* (2013-14); *FCC – Distinguished Visiting Scholar* (2010-2011); *University of Pennsylvania: Annenberg School for Communications (Visiting Scholar 2008-2018)*

**Covington & Burling, LLC**. Washington D.C. 1993-2009  
 Of Counsel (02-09), Partner (00-02), Associate (93-00)

Helped manage communications and information policy practice, client relations and development, strategy, training, pro bono, diversity initiatives. Advised communications companies, industry associations, entrepreneurs, venture funds, journalists, governments, and nonprofit entities on U.S. and European law and policy. Handled billing, budgeting.

- Developed foundational FCC, EU, legislative policies on digital services, spectrum management, information technology, public media
- Litigated challenges to communications rules and statutes
- Drafted licensing, programming, distribution agreements

**U.S. Federal District Court**. Philadelphia. Law Clerk to Judge Norma L. Shapiro 1992-1993

**Bar Memberships**: PA, DC. **Boards**: Hazon **Personal**: Married, three kids, yoga, cycling, kayaking.

***Book under contract (Oxford University Press):*** Algorithmic City***Law Reviews***(some available at [SSRN](#))

1. *Information Fidelity*, KNIGHT-COLUMBIA FIRST AMENDMENT PAPER (forthcoming 2020)
2. *Urbanism Under Google: Lessons from Sidewalk Toronto*, 88 FORDHAM L. REV. 457 (2019) (with Julia Powles)
3. *Defining Equity in Algorithmic Change*, REGULATORY REVIEW (2019)
4. *Algorithmic Transparency for the Smart City*, 20 YALE J. OF LAW & TECH. 103 (2018) (with Robert Brauneis)
5. *Zero Rating Broadband Data: Equality and Free Speech at the Network's Other Edge*, 15 COLO. TECH. L. J. 63 (2016)
6. "Smart Cities" Meet Anchor Institutions: Public Libraries and Broadband, 41 FORDHAM URBAN L. J. 1665 (2014)
7. *Visual Gut Punch: Persuasion, Emotion, and the Constitutional Meaning of Graphic Disclosure*, 99 CORNELL L. REV. 513 (2014)
8. *Modeling Policy for Public Media*, 24 HARV. J. OF LAW & TECH. 112 (2010) (with Anne H. Chen)
9. *Digital Public Service Media Networks to Advance Broadband and Enrich Connected Communities*, 9 J. TELECOM & HIGH TECH. L. 82 (2010) (with Anne H. Chen)
10. *Spectrum Auctions and the Public Interest*, 7 J. TELECOM & HIGH TECH. L. 343 (2009)
11. *No Time for Equal Time*, 76 GEO. WASH. L. REV. 897 (2008) (symposium issue)
12. *Free Speech and Media Policy: The First Amendment at War With Itself*, 35 HOFSTRA L. REV. 1211 (2007) (symposium issue)
13. *Peer Promotions and False Advertising Law*, 58 S. CAR. L. REV. 683 (2007) (symposium issue)
14. *Animal Ethics and the Law*, 79 TEMPLE L. REV. 1291 (2006) (book review)
15. *Stealth Marketing and Editorial Integrity*, 85 TEX. L. REV. 83 (2006)
16. *Spectrum Equity*, 4 J. TELECOM. & HIGH TECH. L. 101 (2005)
17. *Media Policy Out of the Box: Content Abundance, Attention Scarcity, and the Failures of Digital Markets*, 19 BERKELEY TECH. L. J. 1389 (2004)
18. *Spectrum Rights in the Telecosm to Come*, 41 SAN DIEGO L. REV. 269 (2004)
19. *Tender Justice: Judge Norma L. Shapiro's Hard-Headed Humanity*, 152 U. PA. L. REV. 25 (2003)
20. *Bargains in the Information Marketplace: The Use of Government Subsidies to Regulate New Media*, 1 J. TELECOM. & HIGH TECH. L. 217 (2002)

21. *Digital Television and the Allure of Auctions: The Birth and Stillbirth of DTV Legislation*, 49 **339** COMM. L.J. 517 (1997)

### ***Book Chapters and Monographs***

1. *Smart City Ethics*, in OXFORD HANDBOOK OF THE ETHICS OF ARTIFICIAL INTELLIGENCE (forthcoming 2020)
2. *Report of the Media Subcommittee for the Study of Digital Platforms*, George J. Stigler Center for the Study of the Economy and the State The University of Chicago Booth School of Business (July 2019) (co-author)
3. *The Atomic Age of Data: Policies for the Internet of Things*, Aspen Institute Report (2015)
4. *Public Media Policy Reform and Digital Age Realities* in COMMUNICATIONS LAW AND POLICY IN THE DIGITAL AGE: THE NEXT FIVE YEARS (Randolph May ed.) (Carolina Academic 2012)
5. *Public Service Media Narratives* in HANDBOOK OF MEDIA LAW AND POLICY: A SOCIO-LEGAL EXPLORATION (Monroe E. Price & Stefaan G. Verhulst, ed.)(Routledge 2012)
6. INFORMATION NEEDS OF COMMUNITIES (Steven Waldman, ed.) (Carolina Press 2011) (principal author of 50 page nonprofit media section)
7. *Spectrum Policy and the Public Interest* in TELEVISION GOES DIGITAL (Darcy Gerbarg ed.) (Springer 2009)
8. *Public Service Media 2.0* in ... AND COMMUNICATIONS FOR ALL: A POLICY AGENDA FOR A NEW ADMINISTRATION (Amit M. Schejter ed.)(Lexington Books 2009)
9. *Public Television and Pluralistic Ideals* in THE FUTURE OF PUBLIC SERVICE BROADCASTING (Tim Gardam & David Levy ed. (Reuters Institute 2008)
10. *Spectrum Sharing and Spectrum Efficiency* in A FRAMEWORK FOR A NATIONAL BROADBAND POLICY (Aspen Institute 2008)
11. *Proactive Media Policy in an Age of Content Abundance* in MEDIA DIVERSITY AND LOCALISM: MEANINGS AND METRICS (Philip M. Napoli ed.)(Erlbaum 2006)

### ***Press publications***

“Opinion: The more outrageous the lie, the better it is for Facebook’s bottom line,” (with Karen Kornbluh), *The Los Angeles Times* (11/9/19)

“How Facebook Shot Themselves in the Foot in their Elizabeth Warren Spat” (with Karen Kornbluh), *The Guardian* (10/15/19)

“How to Regulate the Internet” (with Karen Kornbluh), *Project Syndicate* (7/10/19)

“Bringing Truth to the Internet: Efforts to treat individual disinformation outbreaks, rather than the underlying systemic design flaws, are doomed to fail. Here’s what we need” (with Karen Kornbluh), *Democracy Journal* (Summer 2019, No. 53)

“Curb its Enthusiasm: As Sidewalk Labs Moves Fast in Toronto, Pay Attention to the Streets,” *Globe and Mail* (6/14/19)

“Reviving the Personal Attack Rule for Digital Platforms is Not a Good Idea,” *Protego Press* (5/28/19)

“The First Amendment Opportunism of Digital Platforms,” *German Marshall Fund* (2/11/19)

“So, Mark Zuckerberg wants to repent for Facebook's sins? He can start here,” *The Guardian* (10/2/17)

“Facebook Should Consider Subsidizing and Promoting Local News,” *Slate* (12/1/16)

“Facebook and Google: most powerful and secretive empires we've ever known,” *The Guardian* (9/28/16)

“Self-driving cars: overlooking data privacy is a car crash waiting to happen,” *The Guardian* (6/8/16)

“Big pharma, tobacco, tech - how the first amendment is being abused,” *The Guardian* (3/16/16)

“India's ban on Facebook's free service is an overreaction,” *The Guardian* (2/8/16)

### ***Works in Progress***

1. *Friction Policy*
2. *Community Benefits Agreements for the Smart City*
3. *The Place of Transparency Amid Information Glut*

### ***Other Periodical Publications***

1. *Prospects for U.S. Spectrum Management*, Practicing Law Institute (2002) (with Stanford McCoy and Devandra Kumar)
2. *Access Through Cable: Who Will Control the Cable Internet Gateway?*, Australian Media Law Association’s COMMUNICATIONS LAW BULLETIN, April 2000
3. *Towards Digital Television and New Paradigms for Media Law and Regulation*, American Bar Association’s BULLETIN OF LAW, SCIENCE AND TECHNOLOGY, December 1997
4. *Second Byte: Congressional Excursion into Digital TV*, American Bar Association’s COMMUNICATIONS LAWYER, Summer 1996
5. *Superhighway Patrol: Why the FCC Must Police the Airwaves*, THE WASHINGTON POST, August 6, 1995

## **SELECTED PRESENTATIONS**

### ***Public Addresses, Podcasts***

1. *Dueling Platform Policies and Free Speech Online*, Constitution Center We The People Podcast (Nov. 2019)
2. *Information Fidelity*, Knight First Amendment Institute Symposium: The Tech Giants, Monopoly Power, and Public Discourse (Nov. 2019)
3. *Facebook, Free Speech, and Political Advertising*, Radio Times WHYY (Nov. 2019)
4. *Digital Governance*, WGBH Boston (Nov. 2019)
5. *Digital Governance in the City*, 2019 Cooper-Walsh Colloquium: Urban Intelligence and the Emerging City, Fordham Law School (Oct. 2019)

6. *A New Digital Agency*, German Marshall Fund Digital Innovation & Democracy Initiative (2019)
7. *Beyond Risk Assessment—Algorithmic Governance in Law Enforcement and Criminal Justice*, Drexel Law School (Sept. 2019)
8. *Artificial Intelligence and Human Rights, Surveillance, and Democracy*, University of Pennsylvania, Perry World House 2019 Global Order Colloquium (Sept. 2019)
9. *Algorithmic Justice*, The Leadership Conference on Civil and Human Rights (Sept. 2019)
10. *Algorithmic Prediction and Law*, (workshop, co-hosted by Cornell University’s AI Policy and Practice Project, Upturn, and the Stanford-based AI100 initiative) (June 2019)
11. *The Disclosure Fix*, International Communications Association Pre-Conference on Datafication (May 2019)
12. *Platform Regulation*, 2019 Antitrust and Competition Conference – Digital Platforms, Markets, and Democracy: A Path Forward (May 2019)
13. *Smart City Ethics*, University of Toronto School of Law (March 2019)
14. *Google’s Urbanism: Sidewalk Labs in Toronto*, Fordham University School of Law (February 2019)
15. *Algorithmic Accountability*, Georgetown Law-Cornell Tech Roundtable on the Political Economy of Data (Dec. 2018)
16. *Algorithmic Accountability*, 3rd Translational Data Science Workshop, New York University (Oct. 2018)
17. *Freedom of Expression and Digital Platforms*, Council on Foreign Relations (June 2018)
18. *Media Law and Digital Platforms*, Antitrust and Competition Conference – Digital Platforms and Concentration, Stigler Center, Chicago Booth Business School (April 2018)
19. *Algorithmic Transparency*, Silicon Flatirons, University of Colorado (Feb. 2018)
20. *Algorithmic Transparency*, Boston University Computer Science Dept. (Nov. 2017)
21. *Algorithmic Transparency*, MetroLab, Washington D.C. (July 2017)
22. *The Future of Public Media*, American Academy of Arts & Sciences, New York (June 2017)
23. *Big Data and Education*, Haifa University School of Law (May 2017)
24. *Algorithmic Accountability for Smart Cities*, The Power Switch: How Power is Changing in a Networked World, University of Cambridge (March 2017)
25. *Open Records Laws and Algorithmic Accountability*, What Works Cities 2017 Summit, New York (March 2017)
26. *Fake News*, Yale Information Society Project (Feb. 2017)
27. *Weaponizing Information*, Yale Information Society Project (Jan. 2017)
28. *Informational Privacy*, Annual Meeting of Pennsylvania Trial Lawyers, Hershey, PA (July 2016)
29. *Markets, Innovation and Regulation*, Fordham Law School (May 2016)
30. *Risk and Resilience in Technology Regulation*, University of Arizona Law School (May 2016)
31. *Native Advertising Public and Private Policies*, Cardozo Law School (Feb. 2016)
32. *Zero Rating and Free Expression*, Silicon Flatirons, University of Colorado (Jan. 2016)
33. *Right to be Forgotten and Digital Platforms*, Hearsay Culture Radio (Jan. 2016)
34. *Right to be Forgotten and Digital Platforms*, Wharton Business Radio, The Digital Show (June 2015)
35. *The Meanings of Transparency*, Cyberlaw Colloquium, University of Pennsylvania (May 2015)



36. *Internet of Things: Civil Liberties and Civic Inclusion*, State of the Net Conference, News342 (April 2015)
37. *Comment on Monroe Price, Globalization and Freedom of Expression*, University of Pennsylvania, Annenberg School of Communication (April 2015)
38. *Evolving Legal Standards of "Who's a Journalist,"* in Quality Journalism in the Digital Age Conference, Rutgers University (April 2015)
39. *Algorithms as Editors*, in Digital Intermediaries: Measurement, Monitoring and Theories of Harm, London School of Economics (March 2015)
40. *Right to Be Forgotten*, Cardozo Law School (Jan. 2015)
41. *Policies for the Internet of Things*, Jerusalem Center for Ethics (Dec. 2015)
42. *Spectrum Issues*, Current Issues in Internet Law in Europe and the U.S. MaCCI & CTIC Telecommunications Workshop (April 2014)
43. *Native Advertising and Media Ethics*, London School of Economics (Mar. 2014)
44. *Editorial Independence, Transparency, and Governance*, London School of Economics (Mar. 2014)
45. *Anchor Institutions and Broadband*, Fordham Law School Smart Cities Conference (Feb. 2014)
46. *Spectrum and Public Value*, London School of Economics (Jan. 2014)
47. *The Public Interest and Digital Discourse*, Haifa University School of Law (Nov. 2013)
48. *Fourth Estate Anxieties*, City University of London Department of Sociology (Oct. 2013)
49. *Communications Access Economics*, Public Knowledge Seminar for U.S. Congress, Washington D.C. (June 2013)
50. *Lessons from Broadcast Regulation for the Twenty-First Century*, Administrative Law Review, Washington D.C. (Apr. 2013)
51. *Tobacco Warning Labels and the First Amendment*, Annenberg School of Communication, University of Pennsylvania (Apr. 2013)
52. *Public Media in the Digital Age*, National Press Club (Jan. 2013)
53. Organized and Moderated *Future of New Jersey Public Media*, New Brunswick, NJ (Jan. 2013)
54. *Public Interest Narratives in Spectrum* at Looking Back to Look Forward: The Next Ten Years of Spectrum Policy, University of Colorado Silicon Flatirons, Washington D.C. (Nov. 2012)
55. *The Innovation Narrative in Public Media*, at the Public Service Media and Exposure Diversity Conference, IViR, University of Amsterdam (Sept. 2012)
56. Organizer/Moderator for Ford Foundation Convening on the *Future of the Public Interest in the Post-Broadcast Era* (July 2012)
57. Organizer/Moderator for *The Future of the Public Interest in the Broadband Age*, Rutgers Institute of Information Policy & Law and New America Foundation (May 2012)
58. *Media Policy as Innovation Policy* at Redefining Diversity in a Digital Age: Meeting Information Needs of Communities, Annenberg School, University of Southern California (Jan. 2012)
59. *Content Futures: Who Will Be Content King*, Telecommunications and Media Forum, Washington D.C., (Dec. 2011)
60. *The Future of Public Media*, Free State Foundation Conference (Oct. 2011)
61. Harvard University School of Law, Participated in Conference on the 50<sup>th</sup> Anniversary of Newt Minow's Vast Wasteland Speech (Oct. 2011)
62. Oxford University Center for Comparative Media Studies, Seminar on Media Policy Interventions and the Future of Public Media (July 2011)

63. University of Southern California Annenberg School for Communication & Journalism ~~343~~  
Colloquium on Measuring Participation in the Broadcast, Telecommunications and Digital Media  
Industries (May 2011)
64. *Public Media and Political Influence: Lessons for the Future of Journalism from Around the  
World*, New York University (Feb. 2011)
65. *Wireless Rights Definitions, The Unfinished Radio Revolution: New Approaches to Handling  
Wireless Interference*, The Information Technology and Innovation Foundation (Nov. 2010)
66. *Spectrum Policy and Public Media*, Brookings Institute (Oct. 2010)
67. *Spectrum Policy and Auction Revenue*, New American Foundation (Sept. 2010)
68. Testimony before the New Jersey Legislative Task Force on Public Broadcasting (Sept. 2010)
69. *Public Media, NJN and the Future of Journalism in New Jersey*, Rutgers Eagleton Public Policy  
Institute (Sept. 2010)
70. *Spectrum Policy*, White House meeting on spectrum legislation (August 2010)
71. *Future of Media*, Keynote Address, Progress and Freedom Foundation (May 2010)
72. *Broadband Policy*, Address to the Board of the Corporation for Public Broadcasting (Jan. 2010)
73. *Public Media Policy and the Future of Journalism*, Association of American Law Schools Midyear  
Convention (Jan. 2010)
74. *Policy Directions for the New Public Media*, University of Colorado Silicon Flatirons  
Telecommunications Institute (Jan. 2010)
75. *Public Media in the New Information Ecology*, New School Conference on Internet as Playground  
and Factory (Nov. 2009)
76. *Public Media: From Broadcast to Broadband*, Yale Law School Knight Law and Media Program,  
Conference on Journalism and the New Media Ecology (Nov. 2009)
77. *Public Media: From Broadcast to Broadband*, Harvard Law School Berkman Center for  
Information Policy (Nov. 2009)
78. *Public Media and Sustainability*, Ford Foundation Convening, American University (Nov. 2009)
79. *Public Media and Health Care*, Ford Foundation Convening, Paley Center for Media (Nov. 2009)
80. *Public Media and Education*, Ford Foundation Convening, Paley Center for Media (Oct. 2009)
81. *Green Marketing and the Administrative Agencies*, American Bar Association, Consumer  
Protection Conference (June 2009)
82. *Public Service Media 2.0*, Federal Communications Commission (May 2009)
83. *New Policy Directions in Public Media*, Ford Foundation (April 2009)
84. *Lifecycle Analysis and Public Policy*, Wharton Initiative for Global Environmental Leadership  
(Mar. 2009)
85. *Public Service Media 2.0*, Free State Foundation Roundtable at the National Press Club (Feb. 2009)
86. *Public Service Media 2.0*, New America Foundation (Jan. 2009)

87. Expert panelist for *Reforming the Federal Communications Commission*, National Press Roundtable (Jan. 2009) 344
88. *Pointing the Finger: How Should Governments Assign Liability to Promote the Success of Next Generation Radio Technology*, Software Defined Radio Forum (Oct. 2008)
89. *Green Marketing and Information Policy: The Case of Animal Products*, IT Colloquium, New York University Law School (Oct. 2008)
90. *Public Media in the Networked Environment*, Haifa Law School (May 2008)
91. *Information and the Information Economy*, Fordham Business School (May 2008)
92. *The Future of Public Service Media*, address to the Board of the Public Broadcasting System (Mar. 2008)
93. *Private Rights and Public Broadcasting*, WGBH-TV (Mar. 2008)
94. *The Public Interest in Spectrum Allocation*, The Columbia Institute for Tele-Information, Columbia Business School (Nov. 2007)
95. *Media Ownership*, before the Israel Second Broadcast Authority (Nov. 2007)
96. *Advertising, Communications and Web 2.0*, Haifa University School of Law (Nov. 2007)
97. *Public Broadcasting and Intellectual Property Rights*, American University School of Law (Oct. 2007)
98. *Legal Issues in the New Media Environment*, National Geographic Society (Oct. 2007)
99. *Media Access and the New Intermediaries*, George Washington University School of Law Symposium on Access to the Media: 1967-2007 and Beyond (Oct. 2007)
100. Expert panelist for Aspen Institute Roundtable on Spectrum Policy, Toward a National Broadband Policy: Spectrum Goals and Policies (May 2007)
101. *Regulation for Convergence and Public Service Media in the New Media Environment*, featured speaker at conference on Communication Policy Regulation in the Age of Convergence: From Global to Thai Experience (organized by the Faculty of Communication Arts, Chulalongkorn University) Bangkok, Thailand (May 2007)
102. Expert panelist for CTIA-University of Colorado Public Safety Roundtable, Washington D.C. (Apr. 2007)
103. *Process Objections to Media Concentration*, Commentary on C. Edwin Baker, Media Concentration and Democracy, University of Pennsylvania School of Law (Apr. 2007)
104. *Reclaiming the First Amendment for Media Policy*, Keynote Speaker, Hofstra University Law School (Jan. 2007)
105. *Spectrum Dispute Resolution*, University of Pennsylvania Annenberg School of Communication, Philadelphia (Nov. 2006)
106. *The Future of Broadband Video: A U.S. European Comparative Analysis*, New York Law School and Council of Europe, New York (Sept. 2006)
107. Expert panelist for the National Academies meeting on Spectrum Markets, Washington

108. Expert panelist for the National Academies meeting on Radiofrequency Spectrum Management, Washington D.C. (Aug. 2005)
109. Expert panelist for the National Science Foundation Workshop on Future Spectrum Technology and Policy, Washington D.C. (May 2005)
110. *Spectrum Governance*, AEI-Brookings Joint Center, Washington D.C. (Apr. 2005)
111. *The Broadcast Flag: Administrative Control over Digital Rights Management*, New York University Law School (Mar. 2005)
112. *New Media Policy Goals*, "Democratic Principles in Media Policy for the 21<sup>st</sup> Century," Fordham University (Jan. 2005)
113. *Digital Television Technology and Law*, Georgetown University Law Center, Washington D.C. (Feb. 2004)
114. *Spectrum: The New Battle Front*, MSTV 17 Annual Television Conference, Washington D.C. (Oct. 2003)
115. *Digital Television: Fact or Fiction*, Howard M. Squadron Program in Law, Media & Society and Benjamin N. Cardozo School of Law, in conjunction with the Stanhope Center for Communications Policy Research (Nov. 2002)
116. *The Changing Law of Spectrum: How Should Spectrum Regulation Respond to the Convergence of Wireless Services?*, "Telecommunications Convergence Conference," Practicing Law Institute, New York (May 2002)
117. *Rules of the Road for Digital Transition*, ABA Conference, Las Vegas (Apr. 2002)
118. *The Development of Broadband and the Open Access Challenge*, Conference of the American Society of Engineering Management, Washington, D.C. (Oct. 2000)
119. *Legal Issues Surrounding Digital Television*, WETA-TV/National Telecommunications Infrastructure Administration Conference, Arlington, VA (Oct. 1999)
120. *Broadcast Regulation and the Administrative Process*, George Mason University Law School (Apr. 1998)
121. *U.S. Spectrum and Broadband Policy*, Israel Science and Technology Commission Conference on Technology Commercialization: Managing Intellectual Property, Tel Aviv (Mar. 1998)
122. *Press Freedoms Under U.S. and International Law*, International Research and Exchange Conference on Media Law, Belarus (Sept. 1997)
123. *Defamation and Libel Under U.S. Law*, Slovak Syndicate of Journalists Conference on Media Law, Bratislava (Apr. 1997)
124. *Developments in Video and Internet Services*, 15<sup>th</sup> Annual Practicing Law Institute/Federal Communications Bar Association Institute on Telecommunications Policy and Regulation, Washington, D.C. (Dec. 1997)
125. *The Crucial DTV Allotment/Assignment Process*, Convention of the National Association of Broadcasters, Las Vegas (Apr. 1997)

126. *The U.S. Policy on Digital Television, Brookings Institution's Inside Washington: Focus on Information Superhighway, Washington, D.C. (May 1996)* 346
127. *The FCC and New Technologies, Imperial College of Science, Technology and Medicine, New York City (Oct. 1996)*

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 ELLEN P. GOODMAN**

**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

*EPG*