

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

**B E T W E E N:**

**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, Zeynep Tufekci, of the City of Chapel Hill, in the State of North Carolina, in the United States of America, MAKE OATH AND SAY:

1. I am an associate professor at the University of North Carolina, Chapel Hill at the School of Information and Library Science. I am a contributing opinion writer at the New York Times, and a faculty associate at the Berkman Klein Center for Internet and Society at Harvard University. My research interests revolve around the intersection of technology and society and my academic work focuses on social movements and civics, privacy and surveillance, and social interaction.

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 any 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** at the City of Chapel Hill, in the State of North Carolina on June 4, 2019. *Orange County*

*Yma Benoit Petit Leune*

Commissioner for Taking Affidavits

*Yma Benoit Petit Leune*  
*(or as may be)*

*Zeynep Tufekci*

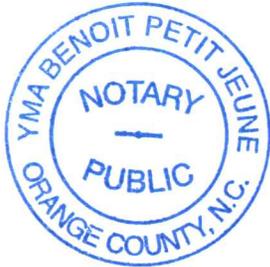
Zeynep Tufekci



MY COMMISSION EXPIRES: *12/11/2020*

This is Exhibit "1" referred to in the Affidavit of Zeynep Tufekci  
sworn June ....., 2019.

*Yma Benoit Petit Jeune* 06/04/2019 State of N.C.  
County of Orange  
\_\_\_\_\_  
Commissioner for Taking Affidavits (or as may be)  
*Yma Benoit Petit Jeune*



MY COMMISSION EXPIRES: *12/11/2020*

**Expert:**

Zeynep Tufekci

May 31, 2019

Associate professor at the University of North Carolina, Chapel Hill

Faculty Associate, Harvard Berkman Klein Center for Internet and Society

Contributing Opinion Writer, New York Times

Prepared for:

Young Park

Fogler, Rubinoff LLP

77 King Street West

Suite 3000, P.O. Box 95

TD Centre North Tower

Toronto, ON M5K 1G8

**Scope of work**

*Documents relied on:*

- Waterfront Toronto: Request for Proposals
- Sidewalk Labs: Approach to Data Privacy
- Sidewalk Labs: Response to Request for Proposals
- Waterfront Toronto & Sidewalk Labs: Presentation: Digital Governance
- Sidewalk Labs: Digital Strategy Advisory Panel Technology Update
- MaRS Solution Lab Primer on Civic Digital Trusts
- Waterfront Toronto BoD Meeting Minutes
- Panel Meeting Minutes
- Presentation – Sidewalk Toronto Responsible Data Use
- Panel Meeting Minutes
- Presentation – Draft Proposals Regarding Data Use and Governance
- Presentation – Civic Labs: Proposed for Discussion

**I have been instructed to consider the following issues:**

1. Are there grounds for concern about privacy breaches in respect of the captured private information, whether or not de-identified, and if there are grounds, do the materials reflect sufficient awareness of and preparation for such breaches?
2. Are the provisions for consent to the capture of private personal information within Quayside adequate, and will it be possible in light of the known facts to ensure meaningful consent by individuals to the capture and use of their personal private information?
3. Are the assurances that the captured personal data will be secure adequate to allay concerns of its use in such a way as to violate privacy?

**Background**

Sidewalk Labs, a Google affiliate, is planning to build in the Quayside area in Toronto's waterfront, a smart city described as "built from the Internet up". This would first be on a 12 acre lot that is currently not developed for residential or business use and primarily owned by Waterfront Toronto, a corporation that was established by the province of Ontario and the city of Toronto as well as the government of Canada. Known as Quayside, it appears to be part urban development project and part a digital/physical experiment. The plan is to scale the same ideas to the 800+ acre eastern waterfront area.

The project has many attractive qualities: it is supposed to be designed to be a walkable city with mixed-income housing. The plans reviewed incorporate good ideas from urban planning experts such as mixed-use areas where residential and business functions can co-exist, public transportation and biking and walking paths, multi-weather environments and more.

However, perhaps the most significant expression of what Sidewalk Labs would be is that it has an extensive digital layer as well as a physical layer that is aimed to be integrated throughout. The plans describe the digital layer, which would include sensors that appear to be everywhere in the city from houses to garbage cans to traffic lights to common areas to underground, as providing "smart city" functions. (See documents Sidewalk Labs: Approach to Data Privacy, Sidewalk Labs: Response to Request for Proposals, and Waterfront Toronto & Sidewalk Labs: Presentation: Digital Governance).

## EXPERT OPINION EXECUTIVE SUMMARY

Data capture of Quayside’s proposed scale and scope naturally raises deep concerns about privacy and surveillance. Sidewalk Labs has published data governance and privacy principles. Sidewalk Labs documents reviewed make “Responsible Data Use” promises around four key areas<sup>1</sup>:

1-Privacy “is about individual control over how personal information is collected, used and shared.”

2-Data Stewardship “is about the use, control, ownership and storage of data.”

3-Access to Data “deals with questions of how broadly and on what terms data is made available”

4-Data Security “is about protecting data and minimizing the potential for breaches.”

These goals are good and laudable goals. Unfortunately, for all four goals, there aren’t convincing, detailed plans about how these goals could be achieved. It’s unclear even if it is possible to achieve these goals given the current level of available technology and methods. There is little discussion of troubling realities in the technology industry, and how they affect these goals. Further, there is little to no discussion of the fact that these goals are in conflict with one another in various ways and potentially not achievable at the same time.

First, the documents available do not provide sufficient details of \*how\* each of these goals will be achieved. There is shockingly little detail on each issue and a lot of “best practices will be followed” type reassurances are sprinkled through the many documents with no detailed discussion appropriate for the scale and the scope of the goals and challenges.

There is also little to no discussion of the current reality. The digital technology industry has been rampant with data breaches, privacy violations, fig-leaf consent procedure, etc. Given this reality of digital technology in the world, there would need to be a lot more detail about how this project would actually be different and actually achieve these goals, or even convince policy-makers and city residents that these goals are achievable.

Second, some of these goals, like data accessibility and privacy, are in direct conflict with one another. If data is provided to third parties even in “anonymized” form, meaning personally-identifiable information has been removed, it’s quite possible that the data will be re-identified, as there have been many such cases (see the main body of this document for more discussion). Further, sharing data with third parties has been a reason for multiple massive data leaks and privacy violations—see the Cambridge Analytica scandal with Facebook, for example. The data could be so stripped that it is harder to re-identify, but that would defeat the purpose of third party data-access, which was to ensure that this rich dataset doesn’t simply become absorbed only by Google which is already a dominant player. This inevitable trade-off is not at all considered in the Quayside document as far as I can tell. This is a striking omission.

---

<sup>1</sup> June 7th, 2018 Sidewalk Labs presentation on Responsible Data Use document.

Third, “meaningful consent” is only meaningful if it is possible to opt-out of the surveillance and the pervasive data collection and still be assured of meaningful participation in the life of this town. Like many other areas, it’s not even clear what meaningful consent would look like, which is a fairly significant omission. But even if we assume that the consent process gets described in better detail, there are significant concerns. The documents provide no description of what happens to the person who does not want to consent given pervasive data collection undergirds every aspect of life. What about visitors? People who work there or travel there for temporary work reasons? Children who cannot consent? There is no assurance that consent will be collected in a way that’s meaningful, let alone that it is even possible to have meaningful consent in such an environment.

Finally, this project assumes that more data is better, that this is an obvious fact, and that all the downsides of pervasive data collection and surveillance can be managed. Given that this has not been demonstrated at all in practice, treating massive data collection as a minor issue that can be taken care of with principles that sound good but are not detailed or substantive is not a promising sign that this project has had a reasonable review of these important questions.

In sum, we can answer the questions by saying important concerns remain on all areas. For question one: There are significant grounds to fear privacy breaches and violations, and the materials do not provide sufficient grounds for confidence in this area. For question two: Consent processes are strikingly underdeveloped and ill-defined, and it’s not even clear that meaningful consent is possible in a pervasive surveillance environment. For question three: data security fears remain and are substantive, especially since data will be shared with third parties (even if de-identified), potentially moved outside of Canada into different jurisdictions, and since data security violations are unfortunately very common.

## **SPECIFIC CONCERNS:**

In this section, I will go into more details of these concerns.

### **Privacy and de-identification concerns:**

One key privacy protection proposed in the documents appears to be de-identification of personal data, which means that data that would point to a person would be stripped of the pointer. In research literature, that is also referred to as anonymizing data. The plan appears to differentiate between personally identifying information and non-personally identifying information, and to keep the latter and make it accessible to third parties via programming interfaces (called API). Making it accessible to third parties is supposed to counter the dangers of monopolization of this data at the hands of a dominant company such as Google. Data that was once personally-identifiable is thus assumed to be releasable to third-parties once anonymized.

### **De-identification is an insufficient protection.**

First, de-identification of data (or anonymization of data) is no longer a sufficient protection of personal data in the age of big data. This is an issue above and beyond the many other questions data collection of this scope and scale raises about data breaches, security errors, etc. which will be addressed later.

There have been many examples of re-identifying (de-anonymizing) purportedly anonymous data by combining public data sources with whatever data that had been released under the false assumption that it was not personally identifiable. For example, researcher Latanya Sweeney's dissertation from MIT in 2001 shows a wide range of "attacks" that combine "anonymously" released medical records with actual people using similarities in voter databases and other such information.<sup>2</sup> In her particular case, the de-identification included some data such as age or gender that had helped her re-identify subjects (for demonstration: she did not release the names).

Findings that even partially identifying data could be matched with public records to re-identify subjects moved researchers to try to scrub databases of "identifying" information such as birth date and gender, but that is also not enough.

To explain the problem with claims of anonymization, consider an example from 12 years ago (which, in current computing environment is a long time, but it illustrates how anonymization is insufficient). Perhaps the most well-known case is the case of the Netflix dataset. In 2007, Netflix published 10 million movie rankings by half a million customers after replacing names with random numbers as a part of a prize for the best recommendation algorithm--a program that

---

<sup>2</sup> Sweeney, Latanya. 2001. Computational disclosure control : a primer on data privacy protection. <https://dspace.mit.edu/handle/1721.1/8589>

would figure out what movie to recommend to someone who had just watched a particular movie. Such algorithms are important as they can keep people on these sites longer. (YouTube, also owned by Google's parent company, Alphabet, utilizes such algorithms, too). Arvind Narayanan and Vitaly Shmatikov of University of Texas at Austin were able to deanonymize some of these users by comparing their timestamps and rankings with another database of movie rankings, that of the Internet Movie Database (IMDB).<sup>3</sup> They also showed that their de-anonymization method would work with as few as eight movie ratings, and even if there were significant errors introduced in the timestamps. In other words, for some users, anonymized data was not at all hard to de-anonymize.

As the same authors later recounted in an article (published in the *Communications of the ACM* June 2010, Volume 53, No:6)<sup>4</sup>, given enough data and publicly available data, the distinction between "identifying" and "non-identifying" attributes is no longer as protective as one might originally believe. For example, one's shoe size and one's purchase of a luggage set on June 1st, 2018 (a completely random date picked as example) may seem like non-identifying information: there are lots of people with a particular shoe size, indeed millions, and lots of people purchase luggage every day. Under most current definitions of "personally-identifiable information" (or PII which is a legal concept in US jurisprudence) these might not qualify as PII or look like PII. However, once combined, those two data points may well narrow the possibilities to a much smaller subset: and there are certainly databases out there of people's purchases and even physical attributes like shoe sizes which can be inferred from their purchases. If there is one more piece of identifying information, like location, another purchase, or age range for example, seemingly anonymous data may well point to a single person.

Since the Netflix case, many other researchers have shown re-identification and de-anonymizing to be possible in rich datasets. If anything, our techniques have gotten stronger. For example, in 2018, researchers from MIT took two datasets from Singapore that were de-identified. (The databases had the kind of data, location and transportation data, that would be quite similar to the data that would be collected by Sidewalk Labs in Quayside.) The researchers matched these two de-identified datasets, one from a local mobile operator and one from a transportation network to try to see how much of it they could de-anonymize. Strikingly, the MIT researchers "could match around 17 percent of individuals in one week's worth of data, and more than 55 percent of individuals after one month of collected data."<sup>5</sup> The researchers estimated the amount of activity needed to match most users over a week. By "looking at users with between 30 and 49 personal transportation records, and around 1,000 mobile records, they estimated more than 90 percent success with a week of compiled data."

This is a crucial problem with Sidewalk Lab's plan to collect enormous amount of data from all around this neighborhood and then make it publicly available in anonymized format, meaning it

---

<sup>3</sup> Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. 2008 IEEE Symposium on Security and Privacy (sp 2008). doi:10.1109/sp.2008.33

<sup>4</sup> Narayanan, A., & Shmatikov, V. (2010.) Myths and Fallacies of "Personally Identifiable Information." *Communications of the ACM*, June 2010. Doi: 10.1145/1743546.1743558

<sup>5</sup> See <http://news.mit.edu/2018/privacy-risks-mobility-data-1207>

would be stripped of personally identifiable information. The likelihood that this kind of data would eventually be de-anonymized for at least some people is a significant threat, and there is no particular way to solve this in a way that achieves two goals of data governance simultaneously: privacy and access to data by third parties.

One solution would be not collecting this much data. However, it appears that Sidewalk Labs is designed to operate through data collection at every level. For example, they plan to reduce waste by charging people for their garbage, arguing that such accountability systems result in less waste.<sup>6</sup> That may well be true, but that requires collecting highly personal information: a person's trash output, for example, just by itself, could indicate number of guests, personal health, or other variations in one's life. If, for example, this data was de-identified and made accessible to third parties as the Sidewalk Labs documents suggest will happen with much of the data collected, it could be a means of re-identifying the person. Combined with other data, a person whose trash output increased may match with other indicators of guests in a particular time period like more purchases of food, calling taxis to transport more people, etc. Everything in the Sidewalk Labs plan seems to hinge on collecting enormous amount of data on everyone as well as places, locations and physical indicators including noise levels, water usage, traffic, people flow and more.

The other alternative would be to keep this data proprietary, and not share with anyone else. However, the reason this level of data collection was proposed to be opened up to third parties in the first place was that the data is very valuable, and it would be wise to avoid having it become proprietary at the hands of a single corporation, especially one whose business model and technical development in the field of artificial intelligence depends on massive data collection. In other words, not sharing this data would mean that only Alphabet/Google could use such a rich dataset to build better artificial intelligence models. This could create a significant competitive advantage to an already giant and dominant corporation.

The documents I reviewed were sparse on details of the privacy protections besides high-level pronouncements. What details I could find on how Sidewalk Labs would operate indicated that they would use “state-of the art” privacy mechanisms such as federated learning, k-anonymity and privacy by design. These are good principles and techniques but are not sufficient. K-anonymity is a method for reducing re-identifiability<sup>7</sup> but does not fully guard against the re-identification threats explained above. Federated learning means that some of the processing would be done on the machines at the “edge” rather than in centralized databases. This is good in general but it’s just too vague: which processes, for what purposes and when? Privacy by design is not a technique, but a cluster of techniques with varying efficacies and lacking details, it’s not a sufficient guarantee. Given the level of threats, it’s not enough to make these very vague and very broad statements without any accompanying details especially as it is unclear from current level of technological developments and industry practices that the privacy threats are even fully addressable.

---

<sup>6</sup> Sidewalk Labs, Project Vision, also “Managing Solid Waste Wisely: Smart Disposal Chain” in the appendix.

<sup>7</sup> See <https://dataprivacylab.org/dataprivacy/projects/kanonymity/index.html>

Even a guarantee that Sidewalk Labs would not use this data for ad-targeting does not solve this problem. The value of this data goes beyond direct targeting of the people by ads. Such deep behavioral data is very useful for predicting human behavior in ways that can structure new products and develop artificial intelligence models, not just ad-targeting. Google has a range of products that could benefit from this data, ranging from Google Maps to their phones to their home devices such as assistant and Nest (a home thermostat) and more. Google has also been moving into healthcare products, and it is hard to imagine how valuable it is to have such a treasure trove of data at every level of an entire functioning city.

### **Google and NHS data: A Case Study**

In 2014, Google acquired DeepMind, an artificial intelligence company. The New Scientist got a copy of the data-sharing agreement and found that the agreement “gives DeepMind access to a wide range of healthcare data on the 1.6 million patients who pass through three London hospitals run by the Royal Free NHS Trust – Barnet, Chase Farm and the Royal Free – each year.”<sup>8</sup> This will include information about people who are HIV-positive, for instance, as well as details of drug overdoses and abortions. The agreement also includes access to patient data from the last five years.”<sup>9</sup> Consequently, DeepMind, or Google, “held data on millions<sup>10</sup> of Royal Free patients and former patients since November 2015, with neither consent, nor research approval.”<sup>1112</sup>

The United Kingdom Information Commissioner’s Office found that “Royal Free NHS Foundation Trust failed to comply with the Data Protection Act when it provided patient details to Google DeepMind.”<sup>13</sup> As the report states, “The Trust provided personal data of around 1.6 million patients as part of a trial to test an alert, diagnosis and detection system for acute kidney injury. But an ICO investigation found several shortcomings in how the data was handled, including that patients were not adequately informed that their data would be used as part of the test.”

When DeepMind was purchased by Google in 2014 and at first, it was said to be “kept at arm’s length and is said to be run independently.”<sup>14</sup> In 2018, Google announced plans to integrate Deep Mind further into the parent company.<sup>15</sup> Rather than being independent, DeepMind now reports

---

<sup>8</sup> Powles, J. (2016, December 04). DeepMind's data deals raise some serious questions. Retrieved from <https://www.ft.com/content/ddd1478e-b70d-11e6-961e-a1acd97f622d>

<sup>9</sup> See <https://www.newscientist.com/article/2086454-revealed-google-ai-has-access-to-huge-haul-of-nhs-patient-data/>

<sup>10</sup> See <https://deepmind.com/blog/ico-royal-free/>

<sup>11</sup> Powles, J., & Hodson, H. (2017, March 16). Google DeepMind and healthcare in an age of algorithms. Retrieved from <https://link.springer.com/article/10.1007/s12553-017-0179-1>

<sup>12</sup> See <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5741783/>

<sup>13</sup> <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/>

<sup>14</sup> See. Stokel-Walker, Chris. (2018). <https://www.wired.co.uk/article/google-deepmind-nhs-health-data>

<sup>15</sup> Stokel-Walker, C. (2018, November 14). Why Google consuming DeepMind Health is scaring privacy experts. Retrieved from <https://www.wired.co.uk/article/google-deepmind-nhs-health-data>

to Google. It's possible that Google, will never have direct access to patient data, but whatever DeepMind can figure out using this level of rich data will surely benefit the parent company (which is presumably why Google purchased DeepMind in the first place: to benefit from artificial intelligence expertise in the company).

Once within a Google company, the data can well be used to train algorithms that can then give Google a competitive advantage even if the data doesn't get shared with other parts of Google—the algorithms and insights from the data may be used elsewhere even if the data is not. It's not that the NHS/DeepMind project has terrible aims: there may well be benefits to patients in the future, but it also has an effect of entrenching Google's already existing dominance at the expense of potential competition and maybe even the public interest: the data belongs, truly, to the public but the commercial benefits may well accrue to a single company.

This is an important case study as it shows that once data is handed over under vague conditions, it is hard to control exactly where it ends up. As the ICO report states, patients cannot be expected to understand all the uses of their data. "For example, a patient presenting at accident and emergency within the last five years to receive treatment or a person who engages with radiology services and who has had little or no prior engagement with the Trust would not reasonably expect their data to be accessible to a third party for the testing of a new mobile application, however positive the aims of that application may be."<sup>16</sup>

### **Google Policy Changes from Past**

Another important consideration is that companies can change their terms of conditions and their data uses over time. For example, Google has in the past changed its policies, and moved to combining data from different sources in its ecology despite earlier policies of keeping them separate.<sup>17</sup> Thus, a person who had started using Google services under the old privacy policy, assuming that YouTube data would be kept separate from searches, would find themselves in a different setup, where their data would now be merged across Google properties. This was met with alarm by FTC and by EU investigators as well as 36 attorney generals who sent a letter expressing their concern.<sup>18</sup> However, not much was done and it doesn't also seem to have affected Google's revenues or profits. Tech industry usually makes significant privacy changes and then users are confronted with long and detailed legal documents where their only options are to click yes, or be cut off from key platforms that play a significant role in public life such as Facebook or Google's YouTube.

---

<sup>16</sup> See <https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf>

<sup>17</sup> Blagdon, J. (2012, March 01). Google's controversial new privacy policy now in effect. Retrieved from <https://www.theverge.com/2012/3/1/2835250/google-unified-privacy-policy-change-take-effect>

<sup>18</sup> Blagdon, J. (2012, March 01). Google's controversial new privacy policy now in effect. Retrieved from <https://www.theverge.com/2012/3/1/2835250/google-unified-privacy-policy-change-take-effect>

This is an important example because it shows that even massive changes to underlying privacy protections can be done with little recourse for ordinary users and with fairly little consequence for Google since it is so dominant.

## Data Security Considerations

In the various documents reviewed, Sidewalk Labs has promised to keep data secure using state-of-the-art methods. In my opinion, this is an area in which Google has an above average industry track record but even that track record is not a sufficient guarantee of data security, especially for data this sensitive. Google has been involved in relatively few data breaches compared to, say, Facebook but it isn't immune. In fact, unfortunately, there appears to be almost no large company with valuable data that seems to be immune to data breaches despite extensive efforts to keep data secure. The number of data breaches of major companies is too long to list and includes some Google breaches as well.

In the case of Google, the most prominent breach was perhaps the so-called operation Aurora in which Google (along with Adobe and other Silicon Valley companies) was targeted allegedly by China—presumably to hack into Gmail accounts of Chinese and/or Tibetan dissidents.<sup>19</sup><sup>20</sup> This was revealed in the form of an announcement by Google in 2010 where hackers had stolen intellectual property by hacking into the Gmail accounts of these dissidents and activists. This was done using malware and encryption networks to make the hacking activity opaque and invisible to Google staff. These techniques allowed the hackers to access a “remote backdoor” to the computers of these activists and establish a channel of interactivity that looked like an SSL connection. Once valuable data is stored somewhere, the odds of it being attacked go up, and unfortunately, there doesn't seem to be any way to guarantee unbreachable defenses even by companies with the resources and expertise of Google.

More recently, Google shut down its social network, Google+, after discovering itself that a bug had exposed the data of more than half a million Google+ users for about three years.<sup>21</sup> The bug (or error) was that the Google+ API “was not operating as intended.” An API is an interface that connects databases to external parties, and is the same mechanism that Sidewalk Labs is intending to use to share (de-identified) data with third parties. Google CEO Sundar Pichai begun a probe into the API in 2018 called Project Strobe to audit this API or third-party developer access interface which resulted in an internal memo that found the leak of 100,000 private user data points. The leak revealed that there was a bug in the API which allowed third-party developers

---

<sup>19</sup> Connect the Dots on State-Sponsored Cyber Incidents. (n.d.). Retrieved from <https://www.cfr.org/interactive/cyber-operations/operation-aurora>

<sup>20</sup> Zetter, K. (2017, June 04). Google Hack Attack Was Ultra Sophisticated, New Details Show. Retrieved from <https://www.wired.com/2010/01/operation-aurora/>

<sup>21</sup> Newman, L. H. (2018, December 10). A New Google Blunder Exposed Data From 52.5 Million Users. Retrieved from <https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/>

to gain access to personally identifiable information including the names, email addresses, ages, occupations and relationship statuses of 100,000 to up to 500,000 individuals on Google+. (For details, see references 15-17) This was because of access granted to over 400 software applications through the API. The Wall Street Journal gained access to this leak which suggested that Google was unsure of which users were affected or which data had been misused, if at all.<sup>2223</sup> The leak of this internal memo led to the shutdown of Google+ following an announcement by Sundar Pichai on the new data privacy measures Google would unveil and giving Gmail users the ability to limit the data that they wanted to share on an app by app basis.

Also, Google products can include more surveillance than disclosed. For example, Google confirmed in 2019 that its Nest products contain microphones and that this was “an error.” The Google Nest, a series of smart home products including thermostats, smoke detectors and security systems under the Google LLC brand, allegedly neglected to tell users that the microphone was there.<sup>24</sup> This may well have been an error, as Google claimed, but that means that a hacked Nest was a dangerous invasion of a home, allowing the hacker to listen in on conversations, or that a Google error could have accidentally turned it on. Indeed, in 2017, Google admitted that its Google Mini “assistant” was “eavesdropping on users.”<sup>25</sup> In that particular case, Google said it was a hardware flaw but then a spokesperson told Business Insider that not listing the microphone was an oversight instead of a flaw, “the on-device microphone was never intended to be a secret and should have been listed in the tech specs.”<sup>26</sup> Google said that the microphone was not “on” unless users enabled it as such but the incident revealed two core issues: the lack of informed choice for consumers when they purchase products and give up their data, and second, on how and when this data is collected, as well as lack of attention to user privacy and notice. (See references above). This is especially important as similar in-home devices are proposed to be installed in Quayside by Sidewalk Labs.

Also, software can contain bugs and errors. If data is collected and especially if it is valuable, breaches, leaks, hacks and errors are substantial risks.

As disclosure, I do often recommend that journalists, especially in authoritarian countries, use Gmail, a Google product, as their main email unless their “threat models” (or, the parties that could harm them or that they are whistleblowing against) includes Western Governments since

---

<sup>22</sup> MacMillan, D., & McMillan, R. (2018, October 08). Google Exposed User Data, Feared Repercussions of Disclosing to Public. Retrieved from <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194>

<sup>23</sup> Timberg, C., Merle, R., & Zakrzewski, C. (2018, October 08). Google for months kept secret a bug that imperiled the personal data of Google users. Retrieved from [https://www.washingtonpost.com/technology/2018/10/08/google-overhauls-privacy-rules-after-discovering-exposure-user-data/?utm\\_term=.fb154acfe0f8](https://www.washingtonpost.com/technology/2018/10/08/google-overhauls-privacy-rules-after-discovering-exposure-user-data/?utm_term=.fb154acfe0f8)

<sup>24</sup> Snider, M. (2019, February 20). Google mistakenly forgot to tell users that Nest Secure comes with built-in microphone. Retrieved from <https://www.usatoday.com/story/tech/talkingtech/2019/02/20/google-nest-secure-microphone/2925026002/>

<sup>25</sup> Week, L. (n.d.). Google admits its new smart speaker was eavesdropping on users. Retrieved from <https://money.cnn.com/2017/10/11/technology/google-home-mini-security-flaw/index.html>

<sup>26</sup> Kraus, R., & Kraus, R. (2019, February 20). Google accidentally didn't tell anyone about the microphone in its Nest Secure device. Retrieved from <https://mashable.com/article/nest-secure-built-in-microphone-google/>

they can use legal means to get Google data, such as subpoenas and crucially, National Security Letters. In the latter case, Google would provide the data to the United States government but potentially without being able to inform the user that his or her data had just been shared in this particular way.<sup>27</sup> It appears that Sidewalk Labs may take data collected in Toronto to outside of Canada, and store it in other countries, including potentially United States. This would mean that very detailed information about people living in this city could be shared with United States government agencies without disclosure.

## Questions of Consent

I have scoured the documents provided to understand how consent would be possible and meaningful under such a data surveillance regime. There are two separate questions. First, how does consent work? Second, is it meaningful consent?

As with other areas, in the documents reviewed, the details are vague and insufficient. For example, it appears that affirmative consent will be sought for information capture in spaces like homes, but in public areas there will simply be notices of data collection, with icons supposed to indicate whether data is identified or de-identified, and whether the data collected was "image, voice, wave or video".<sup>28</sup> This is very vague considering the depth of information proposed to be collected. (I am not even sure what they mean by "wave"? Audio?)

First, it appears that it is not possible to opt-out of data collection and participate in public places in this city. Is everyone who lives in this neighborhood automatically supposed to consent to surveillance in all public spaces? A delivery person who's bringing something along? A friend visiting a family? Signs informing people of the data collection aren't consent, they are decrees that only serve to inform. Even there, the information is insufficient.

Second, even in areas where individual consent is sought, it might not be possible to meaningfully opt-out. In an environment that is completely dependent on massive data surveillance, it may be impractical and massively inconvenient for a person to withhold consent to surveillance since most basic functions will require participation. It's one thing not to be online in a neighborhood where many others are not; it's another where many basic functions require connectivity and data sharing. For example, Sidewalk Labs envisions that neighborhood meetings and people with similar interests finding one another to be a function of its data streams. How is one supposed to not consent to such functions, if the downside is being left out? Public transportation is supposed to alter its rides depending on who is waiting for it: would that mean that opting out of data collection means inability to use buses? Since trash is charged to households and is analyzed using smart functions, how are people supposed to opt-out of that? Are people who do not want to be surveilled not supposed to walk in the streets? Consent cannot be meaningful without full,

---

<sup>27</sup> See: <https://www.eff.org/issues/national-security-letters/faq>

<sup>28</sup> See Sidewalk Labs documents.

detailed and substantive discussion of how someone can opt-out without suffering a major penalty.

Third, alarmingly, the documents promised to “not share or link personal data with 3rd parties - including other Alphabet companies (i.e. Google) without consent” which means that there may be scenarios that Google would seek consent to use this data, or share it with other third parties. Just raising this possibility is worrisome because it’s possible that people might even consent to this kind of data sharing in return for some conveniences or personal benefits or to obtain benefits (like catching a ride or using neighborhood services which will all be data driven) without being fully able to understand what this data can reveal, therefore being unable to give meaningful consent since they would not have the full information on the power of this kind of data.

Fourth, 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. Meaningful consent has to be informed consent, and given data can reveal more than its surface applications, informing users of the full threat to privacy of this kind of data collection.

To give one, take the case of Strava, a fitness app used by runners has long made the routes of runners’ public if the runner had consented to it. On the surface, this appears like a great idea, and indeed, it is used by many runners to find new routes, whether on their own cities or when they travel. I wrote about this debacle for the New York Times.<sup>29</sup> A relevant excerpt is below:

Since November, Strava has featured a global “heat map” showing where its users jogged or walked or otherwise traveled while the app was on. The map includes some three trillion GPS data points, covering more than 5 percent of the earth. Over the weekend, a number of security analysts showed that because many American military service members are Strava users, [the map inadvertently reveals](#) the locations of military bases and the movements of their personnel.

Perhaps more alarming for the military, similar patterns of movement appear to possibly identify stations or airstrips in locations where the United States is not known to have such operations, as well as their supply and logistics routes. Analysts noted that with Strava’s interface, it is relatively easy to identify the movements of individual soldiers not just abroad but also when they are back at home, especially if combined with other public or social media data.

Apart from chastening the cybersecurity experts in the Pentagon, the Strava debacle underscores a crucial misconception at the heart of the system of privacy protection in

---

<sup>29</sup> Tufekci, Z. (2018, January 30). The Latest Data Privacy Debacle. Retrieved from <https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html>

the United States. The privacy of data cannot be managed person-by-person through a system of individualized informed consent.

In this particular case, every party had given consent, but clearly they hadn't imagined what the data would lead to once analyzed in the aggregate. The military personnel obviously had no intention of outing secret US bases in Yemen or elsewhere, and US Department of Defense officials did not think about warning their soldiers about such apps. Yet, in the end, the result was that the *collective data* revealed a lot more than what individual data users had ever imagined. (Some other countries also had their previously secret base locations revealed through this dataset). The richer the dataset, the truer the theory: collectively, data can reveal more than what we considered when consenting to its collection.

Another danger from collection of this kind of data comes from computational inference. This is a case in which machine learning algorithms can use the data to reveal things that we had not considered.

I wrote about privacy and computational inference, too, in another New York Times article.<sup>30</sup>

Consider another example. In 2017, academic researchers, armed with data from more than 40,000 Instagram photos, used machine-learning tools to [accurately identify](#) signs of depression in a group of 166 Instagram users. Their computer models turned out to be better predictors of depression than humans who were asked to rate whether photos were happy or sad and so forth.

Used for honorable purposes, computational inference can be a wonderful thing. Predicting depression before the onset of clinical symptoms would be a boon for public health, which is why academics are researching these tools; they dream of early screening and prevention.

But these tools are worrisome, too. Few people posting photos on Instagram are aware that they may be revealing their mental health status to anyone with the right computational power.

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. For example, people's waking hours, places they go, how fast they walk, etc. changes in their routines, are potential indicators for many health and mental health events. Even simple analysis of data can reveal a lot. For example, in 2014, Uber, the ride-sharing company wrote a blog post analyzing, for

---

<sup>30</sup> Tufekci, Z. (2019, April 21). Think You're Discreet Online? Think Again. Retrieved from <https://www.nytimes.com/2019/04/21/opinion/computational-inference.html>

example, rides that they called “rides of glory”—meaning people who had gone somewhere new on a Friday night other than their home, and left from there Saturday morning, strongly implying that they had a database of one-night stands in major US cities like DC, Seattle, and more.<sup>31</sup> Location data can likely predict depression or manic episodes, or other health considerations: are you walking more than usual? Less? Things like in-home sensors may provide other clues: are you getting up in the middle of the night? Are the lights on more or less than usual?<sup>32</sup>

Worryingly, such analysis can be done even from de-identified data and then used to understand, or even nudge or try to influence, other people. It may well be possible to collect all this data and not use it in a particular manner that violates individual privacy of these people, but collectively, poses privacy threats to society.

To provide one scenario, this kind of city-wide data could be used to match walking patterns of people with visits to therapists, to gather insights into how walking patterns may be used to predict depression. It might then even delete all the original data, seemingly protecting the privacy of the people from whom this data was gathered but then use the *insights* to do such predictions on other people elsewhere in the world. 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. A company may even mean well and inform users as far as it knows at the moment, but the field is developing very fast. Any kind of rich, continuous and longitudinal data on people is very likely to create important privacy considerations and should be fully considered and discussed.

For example, I recently found out that Google scans all my Gmail account to make a list of all my purchases that it has inferred by reading my emails and figuring out which ones are orders or receipts. I never asked for such a list to be created, and only accidentally found out about it because I am a privacy-focused researcher. Unbeknownst to me, there was an inferred list of my purchases, all in one place. I was genuinely surprised. Such a list is obviously a major privacy danger: if it is hacked or leaked or breached, it would reveal an enormous amount about me. It has no benefit to me, in fact I never asked for it and I don’t know how to opt-out of it despite being an expert. Why did Google compile it? The company hasn’t provided an answer I found satisfactory especially since it is not a feature that is widely known. Presumably, it might help their ad-targeting. It’s also a bigger risk than someone breaking into my email, because they would have to wade through each purchase one by one. Instead, Google has handily provided

---

<sup>31</sup> Tufekci, Z., & King, B. (2014, December 07). We Can't Trust Uber. Retrieved from <https://www.nytimes.com/2014/12/08/opinion/we-cant-trust-uber.html>

<sup>32</sup> For example see: Saeb S, Lattie EG, Schueller SM, Kording KP, Mohr DC. 2016. The relationship between mobile phone location sensor data and depressive symptom severity. *PeerJ* 4:e2537 <https://doi.org/10.7717/peerj.2537> and Farhad et al. 2016. Behavior vs. introspection: refining prediction of clinical depression via smartphone sensing data. <https://ieeexplore.ieee.org/abstract/document/7764553> and Palmius et al. 2016. Detecting Bipolar Depression From Geographic Location Data. <https://ieeexplore.ieee.org/abstract/document/7676335> These are a tiny glimpse of power of data to predict things way beyond what the data originally indicate.

them with a multi-year list, without warning to ordinary users and apparently without much thought about potential downsides.<sup>33</sup>

It's not the first time Google has been unable to predict uses of putting data together with other data. In 2010, Google created Google Buzz, a social network of sorts, and scanned your email contacts in Gmail to have people automatically follow whomever they chat with most, and then making that list public. Of course, this was a privacy nightmare, because it meant that all of a sudden, whomever you were talking with was visible to the whole world. Somehow, Google's engineers hadn't thought of such a basic problem. I don't mean to argue that they are incompetent, but that given complexity of data and what it can reveal, it's very easy to reveal more than one intends very easily.<sup>34</sup>

One solution that has been proposed in Sidewalk Lab's documents is to limit data use to only applications that have been consented to. I could not find any description that would come close to "meaningful consent" let alone assurances that people would fully understand what they were consenting to, and that it would be possible to live in a city that depends on surveillance at such a deep level without consenting to this kind of data collection. If it is inconvenient and difficult to even exist without consenting, then consent is not free or meaningful. Given the way this city seems to be designed, and the vagueness of both privacy protections, data use, data sharing and consent mechanisms, I would not consider this to be a meaningful consent scenario.

The business model of Sidewalk Labs is an important consideration, and may add significant privacy and or surveillance threats or issues. For example, Google has pushed ad-funded kiosks in NYC, and has recently moved to provide ads in taxi cabs in New York.<sup>35</sup> Such methods of ad-targeting become more profitable via targeting and tracking ad-effectiveness. Similarly many Google services such as maps and artificial intelligence applications are improved data. There isn't information in the provided documents on how the Sidewalk Labs effort will make money.

Last but not least, there is also no discussion of the consent as it pertains to minors who might be living in this city or visiting: are parents able to sign off on massive surveillance of children and teenagers? What about a teenager who's visiting a friend who lives there?

## **Conclusion**

The documents reviewed about the Sidewalk Labs project fails to assure that the four goals, privacy, data stewardship, access to data and data security can be achieved as aimed for, especially at the same time.

---

<sup>33</sup> Barrett, B. (2019, May 20). Security News This Week: Oh Great, Google Tracks What You Buy Online With Gmail. Retrieved from <https://www.wired.com/story/google-purchases-gmail-adobe-roundup/>

<sup>34</sup> Wood, M. (2010, February 11). Google Buzz: Privacy nightmare. Retrieved from <https://www.cnet.com/news/google-buzz-privacy-nightmare/>

<sup>35</sup> <https://www.adweek.com/programmatic/hundreds-of-nyc-taxis-are-about-to-go-programmatic-thanks-to-a-funding-boost-from-google/>

The details of each goal are vague and far from reassuring. There are repeated references to laudable goals without sufficient details or convincing plans that these goals are possible. The privacy protections that are proposed are alarmingly under-defined. Given the many questions on whether these protections could actually work at this scale of data collection, it is not possible to conclude that residents could be assured that their privacy would be protected.

Throughout the documents reviewed, there is an implicit assumption that collection of massive data is an important good, and that the downsides and threats of pervasive surveillance are minor inconveniences that can be managed but without a convincing plan that this assumption is at all warranted.

There is no discussion of the fact that many of the aims of this project regarding data security, data privacy and sharing of data with third parties, are in conflict with one another, especially given the number of data breaches that have occurred recently and advances in deanonymization of data. Massive data collection and third-party data sharing increases risks of re-identification. Detailed and rich datasets make the data more valuable for hackers and makes data breaches more significant. The trade-offs and important conflicts in all these areas don't appear to be discussed at all in the documents provided.

The consent process is underdefined, and it is unclear that it is even possible to have meaningful consent if living in Quayside requires pervasive surveillance to function as intended.

In conclusion, it is my opinion that residents of this future city can not be assured that the high-level goals for responsible data use as stated in the documents reviewed are achievable either alone or collectively.

## **ZEYNEP TUFEKCI**

zeynep@technosociology.org

917-651-1942

### **EDUCATION**

University of Texas at Austin, Ph.D., 2004. Dissertation: “In Search of Lost Jobs: The Rhetoric and Practice of Computer Skills Training”

University of Texas at Austin, M.A., 1999. Thesis: “Mental Deskilling in the Age of the Smart Machine”

Istanbul University, Turkey B.A., Sociology, 1995

(Also: Bosphorus University, Turkey. Undergraduate degree in Computer Programming)

### **ACADEMIC EXPERIENCE**

*Associate Professor*, 2016 – Present  
School of Information and Library Science  
University of North Carolina  
Chapel Hill, North Carolina

*Andrew Carnegie Fellow*, 2015-2016  
Andrew Carnegie Fellow in the Social Sciences and Humanities

*Assistant Professor*, 2011 – Present  
School of Information and Library Science  
University of North Carolina  
Chapel Hill, North Carolina

*Adjunct Assistant Professor*, 2011-Present  
Department of Sociology  
University of North Carolina  
Chapel Hill, North Carolina

*Faculty Associate*, 2012-Present  
Harvard Berkman Klein Center for Internet & Society  
Harvard University  
Cambridge, Massachusetts

*Fellow*, 2012-2013  
Center for Information Technology and Policy  
Princeton University  
Princeton, New Jersey

*Fellow*, 2011-2012  
Harvard Center for Internet and Society  
Harvard University  
Cambridge, Massachusetts

*Assistant Professor*, 2008-2011  
Department of Sociology and Anthropology  
University of Maryland Balt. Co.  
Baltimore County, Maryland

*Visiting Assistant Professor*, 2005-2008  
Department of Sociology and Anthropology  
University of Maryland Balt. Co.  
Baltimore County, Maryland

## **HONORS**

O'Reilly Security Defender Award, 2016. (Inaugural) for best practices and effective new approaches to online security.

Andrew Carnegie Fellow, 2015-16, Carnegie Corporation of New York. (Inaugural, national class of 32).

Public Sociology Award. 2014. American Sociological Association. Communication and Information Technology Section.

Honorable Mention. Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square. For Top Paper in the *American Sociological Association* Section for Communication and Information Technology, 2013.

Top Paper Award. "Hope and Hype in Social Mobility: Technology, Jobs and the Dream of Meritocracy." *International Communication Association*, 2005.

## **EXTERNAL GRANTS**

2019-2024 **\$5,000,000** Knight Foundation Grant, to establish The Center for Informed Society with three other UNC co-PIs (to be announced soon, not yet public)

2019-2020 **\$750,000** Luminate Foundation (to be announced in July 2019) (To support research into privacy and surveillance especially with machine learning applications, to work on public health and public sphere aspects in two projects).

2019-2021 **\$660,000** Hewlett Foundation (Algorithms and Society) (Co-PI with Deen Freelon)

2018-2020 **\$274,081** Omidyar Foundation (Impact and Consequences of Encrypted Chat Apps) (sole PI)

2018-2020 **\$75,000** Democracy Fund (Artificial Intelligence and Power: A Conceptual, Empirical and Practical Examination) (sole PI)

- 2017-2018     **\$55,000** Democracy Fund: The Consequences of Artificial Intelligence and Machine Learning for the Public Sphere. (First phase grant, to set up future work)
- 2015-2016.    **\$200,000.** Andrew Carnegie Fellowship. (Inaugural class)
- 2010-15       **\$516,815.** National Science Foundation. Beyond the Deficit Model: Gender Schemas, Computing, Preferences, and IT Career Choices. (Awarded full grant as sole Principal Investigator. Added a UNC colleague as co-PI after moving to UNC-Chapel Hill. Award #1203234)
- 2012-         **\$14,400.** Seed Grant, Odum Institute, University of North Carolina at Chapel Hill (with Neal Caren, Charles Kurzman, and Andrew Perrin)
- 2004-08       **\$539,385.** National Science Foundation, Investigating Gender-Based Differences in Perception and Use of I.T. as Factors in I.T. Career Choice, Award # 0429084. Co-Principal Investigator.

## **BIBLIOGRAPHY AND PRODUCTS OF SCHOLARSHIP**

### **Books:**

**Tufekci, Zeynep.** (forthcoming). *Age of Machine Intelligence* (Temporary title, with Penguin Press).

**Tufekci, Zeynep.** (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protests.* Yale University Press.

Straubhaar, J., Spence, J., **Tufekci Z.**, Lentz, R. (Eds.) (2012). *Inequity in the Technopolis: Race, Class, Gender, and the Digital Divide in Austin.* University of Texas Press: Austin.

### **Refereed Papers/Articles**

**Ashlock Jennifer, Stojnic Miodrag, Zeynep Tufekci (under review at Sex Roles).** "Gender and Video Games in the Path to Computing Careers"

**Ashlock Jennifer, Stojnic Miodrag, Zeynep Tufekci (under review at New Media and Society).** "Where is the gender gap in computing? Comparing differences in skill and self-assessments in a sample of middle school students"

**Tufekci, Zeynep.** (2016). *As the Pirates Become CEOs: The Closing of the Open Internet.* Daedalus. 145 (1), 65-78.

**Tufekci, Zeynep.** (2015). "Algorithmic Harms beyond Facebook and Google: Emergent Challenges Of Computational Agency." *J. on Telecomm. & High Tech. L.*, 13, 203-445.

**Tufekci, Zeynep.** (2014). "Engineering the public: Big data, surveillance and computational politics." *First Monday*, 19(7). doi:10.5210/fm.v19i7.4901

- Tufekci, Zeynep.** (2014). “Big Questions for Social Media Big Data: Representativeness, Validity and Other Methodological Pitfalls.” In *ICWSM '14: Proceedings of the 8th International AAAI Conference on Weblogs and Social Media*.
- Tufekci, Zeynep.** (2014). “Social Movements and Governments in the Digital Age: Evaluating a Complex Landscape.” *Journal of International Affairs*, 68(1). December 2014.
- Tufekci, Zeynep.** (2014). “The Medium and the Movement: Digital Tools, Social Movement Politics, and the End of the Free Rider Problem.” *Policy & Internet*, 6(2), 202–208. doi:10.1002/1944-2866.POI362
- Tufekci, Zeynep.** (2014). “The Social Internet: Frustrating, Enriching, but not Lonely.” *Public Culture*. Volume 72. Winter 2014.
- Tufekci, Z., & Brashears, M. E.** (2014). “Are we all equally at home socializing online? Cybersociality and evidence for an unequal distribution of disdain for digitally-mediated sociality.” *Information, Communication & Society*, 17(4), 486–502. doi:10.1080/1369118X.2014.891634
- Tufekci, Zeynep.** (2013) “‘Not This One’: Social Movements, the Attention Economy, and MicroCelebrity Activism.” *American Behavioral Scientist* 57:848-870.
- Kreiss, Daniel and **Tufekci, Zeynep\*** (equal co-authors) (2013) “Occupying the Political: Occupy Wall Street, Collective Action, and the Rediscovery of Pragmatic Politics.” *Cultural Studies - Critical Methodologies*.
- Tufekci, Zeynep** and Wilson, C. (2012), “Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square.” *Journal of Communication*. doi: 10.1111/j.1460-2466.2012.01629.x
- Tufekci, Zeynep.** (2013) “Pepper-spray and Penguins.” *Juncture* 20(2): 130–32.

**Tufekci, Zeynep** (2012). “Facebook, Youth and Privacy in Networked Publics.” *In Proceedings of the 4th Int'l AAAI Conference on Weblogs and Social Media (ICWSM, 2010)*. AAAI Press. (20% acceptance rate)

**Tufekci, Zeynep** (2010). “‘Who Acquires Friends through Social Media and Why?’ ‘Rich Get Richer’ versus ‘Seek and Ye Shall Find.’” *In Proceedings of the 4th Int'l AAAI Conference on Weblogs and Social Media (ICWSM, 2010)*. AAAI Press. (19% acceptance rate).

Cotten, S. R., Anderson, W. A., & **Tufekci, Zeynep** (2009). “Old wine in a new technology, or a different type of digital divide?” *New Media Society*, 11(7), 1163-1186.

**Tufekci Zeynep** (2008). “Can You See Me Now? Audience and Disclosure Management in Online Social Network Sites.” *Bulletin of Science and Technology Studies*. Volume 11, Number 4, June 2008, pp. 544-564(21).

**Tufekci Zeynep** (2008). “Grooming, Gossip, Facebook and Myspace: What Can We Learn About Social Networking Sites from Non-Users.” *Information, Communication and Society*. Volume 11, Number 4, June 2008 , pp. 544-564(21).

Hou, Weimin, Manpreet Kaur, Anita Komlodi, Wayne G. Lutters, Lee Boot, Claudia Morrell, Shelia R. Cotten, A. Ant Ozok, and Zeynep **Tufekci**, “‘Girls don’t waste time’: Pre-Adolescent Attitudes toward ICT,” *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, ACM Press, 2006, pp. 875-880.

Kaur, Manpreet, Weimin Hou, Wayne G. Lutters, Anita Komlodi, Lee Boot, C. Morrell, Shelia R. Cotten, A. Ant Ozok, and Zeynep **Tufekci**, “‘My Mom is a Cell-Phone Illiterate’ – The Influence of Parental Perceptions on Preadolescent Attitudes Towards ICT,” *Proceedings of the 6<sup>th</sup> ACM Grace Hopper Celebration of Women in Computing*, ACM Press. 2006

Kaur, Manpreet, Weimin Hou, Wayne G. Lutters, Anita Komlodi, Lee Boot, C. Morrell, Shelia R. Cotten, A. Ant Ozok, and Zeynep **Tufekci**, “‘My Mom is a Cell-Phone Illiterate’ – The Influence of Parental Perceptions on Preadolescent Attitudes Towards ICT,”

*Proceedings of the 6<sup>th</sup> ACM Grace Hopper Celebration of Women in Computing*, ACM Press. 2006

### **Book Chapters**

**Tufekci Zeynep (2015).** Authoritarian Use of Social Media. In *Is Authoritarianism Staging a Comeback?* Matthew Burrows and Maria Stephan (Eds). Atlantic Council.

**Tufekci Zeynep (2012).** We Were Always Human. In *Human No More - Digital Subjectivities, Un-Human Subjects and the End of Anthropology*, Neil L. Whitehead and Michael Wesch (Eds.) University of Colorado Press.

**Tufekci Zeynep (2012).** Past and Future Divides: Social Mobility, Inequality and The Digital Divide in Austin During The Tech-Boom. In Straubhaar et al (Eds.) *The Persistence of Inequity in the Technopolis: Redefining the Digital Divide*. University of Texas Press: Austin.

Hartenberger, L., **Tufekci Zeynep (2012).** History of High Tech and the Technopolis in Austin. In Straubhaar et al (Eds.) *The Persistence of Inequity in the Technopolis: Redefining the Digital Divide*. University of Texas Press: Austin.

Straubhaar, J. **Tufekci Zeynep**, Spence, J., Rojas, V. (2012). Digital Inequality in the Austin Technopolis – An Introduction. In Straubhaar et al (Eds.) *The Persistence of Inequity in the Technopolis: Redefining the Digital Divide*. University of Texas Press: Austin.

Spence, J., Straubhaar, J. **Tufekci Zeynep (2012).** Structuring Race in the Cultural Geography of Information, Education, Cultural and Media Resources in Austin. In Straubhaar et al (Eds.) *The Persistence of Inequity in the Technopolis: Redefining the Digital Divide*. University of Texas Press: Austin.

Lenert, E., Christensen, M., **Tufekci Zeynep**, Gustafson, K. (2012). The Digital Divide: The National Debate and Federal and State Level Programs. In Straubhaar et al (Eds.) *The*

*Persistence of Inequity in the Technopolis: Redefining the Digital Divide.* University of Texas Press: Austin.

## **Reports and White Papers**

2015. (co-authored) “The Ethics of Algorithms: from radical content to self-driving cars.”  
White Paper for the Ethics of Algorithms Conference for *the Centre for Internet and Human Rights*.  
[https://www.gccs2015.com/sites/default/files/documents/Ethics\\_Algorithms-final%20doc.pdf](https://www.gccs2015.com/sites/default/files/documents/Ethics_Algorithms-final%20doc.pdf)

**Tufekci, Z.** (2003). *Final Evaluation of the Community Technology Training Center for the Department of Education: Three Year Overview*. Grant evaluation and final overview.

**Tufekci, Z** (2002 and 2001). *Community Technology Training Center Evaluation: Initial Work*. Grant evaluation, Co-authored with Joseph Straubhaar and Sharon Strover and also *The CTTC Processes and Outcomes*. Grant evaluation.

## **Internal Grants**

2017 **\$60,000** UNC Algorithmic Society

2014. **\$1,500**. UNC Travel and Research Award.

2012. **\$3,000**. Duke-UNC Consortium for Middle East Studies. Course Development Award.

2009 **\$6,000**. Maryland Institute for Policy Research Fellowship, UMBC

2009 **\$6,000**. Summer Faculty Fellowship, UMBC

2006 **\$5,000**. Middle school students’ concepts of technology and the self. *Women in Information Technology*. Principal Investigator.

## **REFEREED ORAL ACADEMIC PRESENTATIONS**

(Incomplete list after 2017)

(Single author unless otherwise noted. Selected List).

Social Movements in the Digital Age.. *American Sociological Association*, 2017. Montreal, Canada.

Algorithms that Watch, Judge and Nudge. *American Sociological Association*, 2015. Chicago, IL.

Big Data, Representativeness and Validity. *American Sociological Association*, 2015. Chicago, IL.

Algorithms and Social Control. *Theorizing the Web*. 2015. New York, NYC.

Capabilities of Movements and Affordances of Digital Media: Paradoxes of Empowerment. *American Sociological Association*, 2014. San Francisco, CA.

Social Media and Micro-Celebrity Activism in a Global Context: Changing Dynamics of Attention. *American Sociological Association*, 2013. New York, NYC.

Why We Keep Debating Loneliness: Cyberasociality and Differential Dispositions towards Online Social Interaction. *American Sociological Association*, 2013. New York, NYC.

“Arab Uprisings and Collective Action” in Thematic Session: Assessing the Impact of Social Networking and Mobile Internet Access. *American Sociological Association*, August, 2012. Denver, Colorado.

Social Media and the Dynamics of Collective Action. 2011. AUSACE 2011. Arab-US Association of Communication Educators, Beirut, Lebanon.

A Pro-Active Generation Reacts: Facebook, Privacy and Audience Management. *American Sociological Association*, 2011.

Cyberasociality and the Online Sociality Divide: Third Level Digital Divide? *American Sociological Association*, 2011.

Theorizing the Web, 2011. Faster is Different.

Internet Use and Social Ties of Americans: An Analysis of General Social Survey Data, *American Sociological Association*, 2010.

Internet Use, Gaming and Well-Being. *American Sociological Association*, 2010. (with PJ Rey)

Facebook Makes a Village: Social Capital in the Age of (Online) Community. *American Sociological Association*, 2009.

The Tenacious Body: Surveillance , Triangulation and the Collapsing of Contexts in Online Social Network(ing) Sites. *American Anthropological Association*, 2009.

Gender, Social Capital and Social Network(ing) Sites: Women Bonding, Men Searching. *American Sociological Association*, 2008.

Internet Use and Gender, Race and Class: The Digital Divide in the Era of Youtube and Facebook. *American Sociological Association*, 2008. (with Shelia Cotten)

“A million social imprints: The promise and peril of social media data” Workshop on Challenges and Visions in the Social Sciences, ETH, Zurich. 2008

“Multi-Method Analysis of Social Interaction on Online Social Networking Websites.” *International Network for Social Network Analysis*, 2008.

“Presentation of Self for Everyday Surveillance: On the Internet, Everybody Knows You’re a Dog.” *American Sociological Association*, 2007.

“Emerging Gendered Behavior on Social Network Sites: Negotiating Between the Pull of the Social and the Fear of the Stalker.” *International Communication Association*, 2007

“Pathways to Social Mobility Through Information Technology Skills: An Argument for a Segmented Labor Market Approach.” *American Sociological Association*, 2006.

“More than a Tool?: Gender Differences in Pre-Adolescent Attitudes Toward ICT.” *National Science Foundation Joint Annual Meeting* 2006.

“Skills as Cultural Capital in a Segmented Labor Market,” *American Sociological Association*, 2005.

- “Computer Anxiety and Reproduction of Inequality,” *American Sociological Association*, 2005.
- “Hope and Hype in Social Mobility: Technology, Jobs and the Dream of Meritocracy,” *International Communication Association*, 2005. (Recognized with a Top Paper Award).
- “Technology at the Margins: Race, Nation, Class, and Techno-Cultural Capital,” *International Communication Association*, 2005.
- “The Rhetoric and Practice of Job-Oriented Computer Skills Training: Public Policies and Sociological Theories.” *American Sociological Association*, 2004.
- “Rethinking the Theory Behind Digital Divide Initiatives.” *International Communication Association*, 2002.
- “Workforce Training Programs and Evaluation: Lessons from the Field.” *The Community Technology Network Conference*, 2001.
- “From Linguistics to Evolutionary Psychology: Methodological and Ontological Arguments Against Extrapolation.” *International Society For The History, Philosophy, And Social Studies Of Biology*, 2001.
- “Privacy in the Age of the Internet: A New Tragedy of the Commons?” *Broadcast Education Association*, 2000.
- “As Big Brother Comes of Age, Privacy in Digital Panopticon: Expanding on a Debate Gone Awry.” *International Communication Association*, 2000.

### **Other Academic Presentations**

- Tufekci, Zeynep. (2009). Discussant: “Millennial Makeover: MySpace , YouTube , and the Future of American Politics” *Eastern Sociological Association*.
- Tufekci, Zeynep. (2006). *Methodologies and Social Networking Software Research*. Social Software Symposium at the University of North Carolina, Chapel Hill.

Tufekci, Z., Cotten, S., (2006). *Investigating Gender Differences in IT use among middle school students*. National Science Foundation Joint Annual Meeting

### **TEACHING ACTIVITIES**

Nominated for Deborah Barreau Award for Teaching Excellence at UNC in 2014 and 2015.

#### **Classes taught at UNC:**

- INLS 690-189. Big Data and Society
- INLS 690-189. Ethics of Algorithms and Big Data
- INLS 690-189. Intermediate Selected Topics: Social Media and Society.
- INLS 89-001. First Year Seminar. Social Movements and New Media.
- 2012-2013. On leave at Princeton University. Taught one class: WWS-771b. New Media and Social Movements: New Tools for an Old Game.
- Spring 2012. INLS 697-001. Emerging Topics in Information Science
- Fall 2011. 490-189. Social Media and Society

#### **Classes Taught before Coming to UNC**

- Basic Concepts in Sociology (Introduction to Sociology)
- Research Methods
- Elementary Social Behavior (A sociological twist on social psychology)
- Information and Communication Technologies and Society (honors level seminar course)
- Cyberspace, Culture and Society (graduate level Internet & Society course)
- Performance Assessment & Program Evaluation (Graduate Level Research Methods)
- Media and Society

#### PhD Students:

- Sumita Rege. Looking Beyond: A Study of Blogging and What It Tells Us About Occupations. Graduated August, 2013. (member of committee)
- Chad Morgan. The Work Itself: Job Satisfaction among North Carolina Library and Information Science. Graduated 2104. (member of committee)
- Heather Suzanne Woods. (member of committee)

#### Master's Student:

- Oak Ritchie. Platform Algorithms and Their Effect on Civic and Political Arenas. Spring 2015. MSIS degree.
- Rebecca Bowers. Preventing the Escalation of Violence and Addressing Digital Forms of Abuse: Content Analysis of State Cyberstalking Legislation. Spring 2015. MSLS degree.
- Elizabeth Davidson. Twitter and journalism: Journalists' personal voice and the use of Twitter as a news-sharing platform. A Master's Paper for the M.S. in L.S degree. Fall, 2011 (sole advisor)
- Eric White. New Media in the Newsroom: A Survey of Local Journalists and Their Managers on the use of Social Media as a Reporting Tool. Fall 2011. (co-advisor)

#### Undergraduate Honors Thesis:

- Eliza Hinks. 2015. Unfriending and Unfollowing Practices of College Student Users of Facebook.

## **KEYNOTES (ACADEMIC)**

THIS HAS NOT YET BEEN UPDATED. NUMEROUS KEYNOTES 2015-2018

2015. "Algorithms and Society: Making Decisions in the Face of Uncertainty." 25<sup>th</sup> Annual Conference for Law School Computing (CALICON). Denver, CO. (June 20, 2015).
2015. "Algorithms in our Midst: Information, Power and Choice when Software is Everywhere." Computer Supported Collaborative Work (CSCW). Vancouver, Canada. (March 18, 2015).
2015. "Ethics of Algorithms." Keynote (and whitepaper). Centre for Internet and Human Rights at the Technische Universitat Berlin. (March 10, 2015).
2014. "Researching Out Loud: Public Scholarship as a Process of Publishing Before and After Publishing." Bucknell Digital Collaboration Conference, Bucknell University. Bucknell, PA. (November 15, 2014).
2014. "The Internet as an Antidote to Mainstream Media Failure: Citizen Journalism in Turkey." Knight Foundation / Civic Media Conference. MIT. Cambridge, MA. (June 24, 2014).
2012. "To Understand Big Data, You Need More Humans." International Conference on Collaboration Technologies and Systems. Denver, CO. (May 21, 2012).
2012. Keynote in conversation with Andy Carvin. Theorizing the Web. Washington, DC. April 14, 2012.
2012. "Privacy for a Networked World." Keynote for CHI 2012, SIGCHI Conference on Human Factors in Computing Systems. Vancouver, Canada.

## **SELECTED INVITED TALKS**

### TED Talks:

TED talk on Algorithmic Society and Machine Learning. New York, 2017.

“Machine intelligence makes human morals more important.” TED. Banff, Canada. (June, 2016).

“Online social change: easy to organize, hard to win.” TED Global. Rio de Janeiro, Brazil.  
(October, 2014)

### Other (selected):

Technology in Global Activism, Uprisings and Social Movements. Harvard Kennedy School.  
(October, 2016)

“Machine Gatekeepers”. Rice University. (October 2016)

“Collaborative Intelligence For Making World And Business Sustainable.” Camilo José Cela  
University and Fundación Universidad Empresa. Madrid, Spain. (June 16, 2015).

“Information, Social interactions and Algorithms in a Connected Age” I.T. Littleton Seminar.  
James B. Hunt Jr. Library, North Carolina State University. Raleigh, NC. (June 11,  
2015).

“The Limits of Analytics.” People Analytics Conference, Wharton School, University of  
Pennsylvania. Philadelphia, PA. (April 11, 2015),

“Engineering the Public.” Center for Professional & Applied Ethics. University of North  
Carolina, Charlotte. Charlotte, NC. (April 2, 2015).

“Youth Activism in a Post Snowden World.” South by Southwest. (March 15, 2015).

“Game Changers Talk.” IAPP Global Privacy Summit 2015. Washington, D.C. (March 6, 2015).

”Being a reporter when everyone's a journalist and there's data everywhere.” Investigative  
Reporters and Editors Conference. Philadelphia, PA. (March 5, 2015).

"Networked Protest in the 21st Century: Strengths, Weaknesses and Protester Desires." PS595.  
University of California, Santa Barbara. Santa Barbara, CA. (February 6, 2015).

When Companies Study Their Customers: The Changing Face of Science, Research, and Ethics.  
University of Colorado. Hosted by Silicon Flatirons Center for Law, Technology, and  
Entrepreneurship and the Tech Policy Lab at the University of Washington. (December 4,  
2014).

"#Ferguson: Reporting a Viral News Story." Panel discussion at the Tow Center for Digital  
Journalism, Columbia University. New York, NY. (October 23, 2014).

"Movements in a Connected Age: Better at Changing Minds, Worse at Changing Power?"  
Personal Democracy Forum. New York, NY, (June 5, 2014.)

"Has the Academy Become Too Formal to Matter?" Panel discussion on The Ideas Industry: Is  
the Academy Needed or Wanted? The Fletcher School, Tufts University. Medford, MA.  
(April 29, 2014).

"Gezi Protests and Citizen Journalism in Turkey: How @140Journos Curated, Verified and  
Busted Censorship all under 140 Characters." Co-talk with Engin Onder. Berkman  
Center for Internet and Society, Harvard University. Cambridge, MA. (March 13, 2014).

"Gezi Protests and Citizen Journalism in Turkey: How @140Journos Curated, Verified and  
Busted Censorship all under 140 Characters." Co-talk with Engin Onder. Center for  
Information Technology Policy, Princeton University. Princeton, NJ. (March 6, 2014).

"Regulating Big Data in Urban Governance." Smart Law for Smart Cities conference. Fordham  
Law School, Fordham University. New York, NY. (February 27, 2014).

"Who Tweets for the Ummah? From Clash of Civilizations to Bonds of Humor, from Innocence  
of Muslims to #Muslimrage." Columbia Seminar on Religious Orthodoxy, Censorship &  
Social Media, Columbia University. New York, NY. (March 25, 2014).

- "Disruptive Media: Examining Social-Media Fueled Protest Repertoires from Tahrir to Taksim."  
Columbia Journalism School Colloquium, Columbia University. New York, NY. (March 25, 2014).
- "Transnational information Flows: Revolutions and Repression in the Era of Social Media." An Open World, Science, Technology and Society in the Light of Niels Bohr's Thoughts. University of Copenhagen. Copenhagen, Denmark. (December 6).
- "The Boom-Bust Cycle of Social Media-Fueled Protests" MIT Comparative Media Studies, Massachusetts Institute of Technology. (October 17, 2013).
- "Getting from No to Go: Social Media-Fueled Protest Style From Arab Spring to Gezi Protests in Turkey," Berkman Center for Internet and Society and Harvard University. Cambridge, MA. (October 15, 2013).
- "How Social Media is Changing Government and Governance Around the World" Brookings Institute, Washington, D.C. (November 15, 2013).
- "Debating Data, Privacy and Campaigns." Personal Democracy Forum. New York, NY. (June 7, 2013).
- "Engineering the Public: Public Sphere Impacts of Big Data and Computational Politics." Data-Crunched Democracy: Where Do We Go From Here. Annenberg School for Communication, University of Pennsylvania. Philadelphia, PA. (May 31, 2013).
- "The New Media Ecology and Dynamics of Power: Lessons from Egypt and Beyond." The Role of Media in the Arab Spring and its Aftermath: The Special Case of Egypt. Media@McGill, McGill University. Montreal, Canada. (February 6, 2013).
- "Whoa There, Cowboy: Methodological and Conceptual Pitfalls of Big Data Analytics." Center for Information Technology Policy, Princeton University. Princeton, NJ. (March, 7, 2013).

- “Gezi Uprisings and Getting from No to Go.” The Internet and International Politics: Implications for the United States and Europe. Conference of the Harvard Weatherhead Center for International Affairs. Talloires, France. (June 15, 2013).
- “Is the Internet Good or Bad for Politics? Yes. Let’s talk about How and Why.” La Pietra Dialogues on the theme of “Social Media and Political Participation” organized by the New York University Social Media and Political Participation Laboratory and the Center for New Media and Society. Florence, Italy. (May 11, 2013).
- “Free Speech for Whom?” Panel discussion, Theorizing the Web Conference. CUNY Graduate Center, New York, NY. (March 1, 2013).
- “Who’s Not on Social Media.” Social Computing Symposium 2013: Off the Radar."Microsoft Social Media Symposium. New York, NY. (January 17, 2013).
- “Why <<More>> is Different.” Brookings Institute. Panelist at Technology-Mediated Social Participation, Summer Social Webshop. Washington, DC. (August 23, 2012).
- “Why More is More than Merely More.” Internet at Liberty: Promoting Progress and Freedom, Centre for Internet & Society. Washington DC. Sponsored by Google. (May 2012).
- “Social Media and Arab Uprisings. What Do We Know and Don’t Know.” Re:Publica. Berlin, Germany. (May 2012).
- “From Tahrir to Kony: Social Movements Dynamics and Social Media” Kenan Institute for Ethics. Duke University. Durham, North Carolina. (April 2012).
- “Having Your Say Online: The People's Voice in Authoritarian Contexts.” Georgetown University. March 2012. Washington DC.
- “Election 2012: Campaigns, Coverage & the Internet.” South by Southwest Interactive. 2012. Austin, Texas. (March 2012)
- “From Tehran to Tahrir: What Does Twitter Have to do With Revolution.” BRITE conference. Columbia Business School, Columbia University. New York, NY. (March 5, 2012).

“Syncretic Ecologies of New and Old Power.” Social Computing Symposium. Microsoft Research. New York, NY. January 13, 2012.

“From the Tea Party to Occupy Wall Street and Beyond Personal Democracy.” New York University, New York, NY. (December 12, 2011).

“Social Media and International Solidarity.” Amnesty International. (November, 12, 2011). Boston, MA.

"From Uprisings in the Arab World to Social Unrest in London: The New Media Ecology and Citizen/State Dynamics in the 21st Century." Harvard Kennedy School. Shorenstein Center on the Press, Politics and Public Policy. Cambridge, MA. (October 25, 2011)

“From Tehran to Tahrir: Social Media and Dynamics of Collective Action under Authoritarian Regimes.” Harvard Berkman Center for Internet and Society. Cambridge, MA. (September 27, 2011).

“After the Revolution.” Public Square Squared – How Social Fabric is Weaving a New Era. Ars Electronica. Linz, Austria. (September 6, 2011).

“The Power of Strong Ties; The Power of Weak Ties.” Personal Democracy Forum. New York, NY. 2011

Naval Academy Foreign Affairs Conference. People, Power, Politics in the Internet Age. Annapolis, MD. (April, 2011)

“Negotiating Privacy, Boundaries and Visibility in a Networked World: Why We Need to Move Beyond Opt-in vs. Opt-Out.” Colloquium Speaker for the Computer Science and Electrical Engineering Department. Baltimore, Maryland. 2010.

“The iPad: The ‘Jesus Tablet’ and the Resurrection of Consumer” Digital Dialogues at the Maryland Institute for Technology in the Humanities. College Park, Maryland. 2010. (with Nathan Jurgenson)

“1984, Today – Surveillance, Privacy and Online Social Networks.” Austrian Cultural Forum, New York, NYC. 2010.

“Everyone’s all Atwitter: The Promise and Peril of Social Media.” NASA Colloquium on Information Science & Technology. 2010. Goddard, MD.

“Future of Social Networks.” FutureWeb. Raleigh, North Carolina. 2010.

“On the Internet Everyone Knows You're a Dog: Facebook, Myspace and Life in the 21st Century Village.” Annual Speaker at the Department of Sociology at the College of William and Mary. 2008.

“A Different Kind of Social Physics: Online Communities and the Revolution in the Architecture of Our Social Spaces” Johns Hopkins University, Applied Physics Lab. Colloquium. 2008.

## **PROFESSIONAL SERVICE**

### **Co-Edited Special Issue of Peer-Reviewed Journal**

Tufekci, Z., & Freelon, D. (2013). Introduction to the Special Issue on New Media and Social Unrest. *American Behavioral Scientist*. doi:10.1177/0002764213479376

### **Ad Hoc Reviewer (Selected List)**

- Science
- American Journal of Sociology
- Journal of the American Society for Information Science and Technology
- British Journal of Sociology
- Information, Communication and Society
- Future Internet
- Theory and Society
- New Media and Society
- Bulletin of Science, Technology and Society
- The Sociological Quarterly
- Southern Communication Journal
- International Journal of Internet Science
- Human Communication Research
- National Science Foundation (Panel Reviewer) for Directorate for Computer & Information Science & Engineering, Directorate for Social, Behavioral & Economic Sciences, and Human-Centered Computing (HCC)
- Elsevier Science, book reviewer
- Sage, book reviewer
- Oxford University Press, book reviewer

## Service at UNC

### Assignments, duties, activities at SILS:

- 2017-2018 Personnel committee
- 2016-2017 Undergraduate committee
- 2015-2016 Served on the graduate committee
- 2014-2015 Served on the graduate committee
- 2013-2014 Served on the undergraduate committee
- 2011-2012 Served on the undergraduate committee
- Participant in Edward R. Murrow Program (October-November, 2013)

### Public Talks and Panels at UNC

- 2013, October, 11. Panelist at Chancellor's Installation Event at University Day. Panel on Innovation.
- 2013, October, 25. Center for Media Law and Policy
- 2013, September, 3. Global Protests in Context. *Co-sponsored by the Program in the Humanities and Human Values and the Carolina Center for the Study of the Middle East and Muslim Civilizations.*
- 2013, February 26<sup>th</sup>. The 2013 Emerging Trends in Information Professions Showcase
- 2012, February, 3. *UNC SILS 80<sup>th</sup> Anniversary Symposium.* "Should Librarians Care About Privacy Anymore?"
- 2012, January 26. Global Media and/as Local Politics: Reconfigurations of the Mediatized Middle East and North Africa
- 2012 Interview with UNC Student Radio News Show: Carolina Connection

### **Organizational Service to the Profession**

- Editorial Board: Emerald Studies in Media and Communication. 2013-present
- Program Co-Chair: International Conference on Weblogs and Social Media in Dublin, Ireland, May 2012.
- Organizer: Global Voices Academic Summit in Nairobi, Kenya, July, 2012.
- Participant in NSF-funded Technology-Mediated Social Participation Summer Social Workshop in University of College Park, August of 2012.
- Council Member: American Sociological Association, Communication and Information Technology Section
- Co-Editor of Special issue of American Behavioral Scientist on New Media and Social Unrest. 2012.
- Program Committee, International Conference on Weblogs and Social Media, 2010
- Session organizer American Sociological Association, 2009
- Member, Best Paper Award Committee of Communication and Information Technologies and Society section of the American Sociological Association Conference, 2006.
- Program Committee, International Conference on Weblogs and Social Media, 2009
- Author meets critic session panelist, Eastern Sociological Association, 2009
- Session Organizer American Sociological Association 2009
- Reviewer International Communication Association, 2008
- Session Organizer International Communication Association 2007
- Panel Presider in Eastern Sociological Society 2006
- Member, Book Award Committee of Communication and Information Technologies and Society section of the American Sociological Association Conference, 2006.
- Panel Presider in American Sociological Association Conference in 2005
- Session Organizer in American Sociological Association Conference in 2005
- Session Organizer International Communication Association 2005

- Respondent in American Sociological Association Conference in 2005
- Respondent at the Global Fusion Conference, 2005
- Advisory Board of Annual Editions: Computers in Society

**Membership in Scholarly and Professional Organizations**

American Sociological Association

International Communication Association

## **PRODUCTS OF ENGAGED SCHOLARSHIP (Public Writings)**

### **New York Times op-eds**

Tufekci, Z. (2019a, March 8). Opinion | Zuckerberg's So-Called Shift Toward Privacy. *The New York Times*. Retrieved from <https://www.nytimes.com/2019/03/07/opinion/zuckerberg-privacy-facebook.html>

Tufekci, Z. (2019b, April 26). Opinion | Think You're Discreet Online? Think Again. *The New York Times*. Retrieved from <https://www.nytimes.com/2019/04/21/opinion/computational-inference.html>

Tufekci, Z. (2018a, January 3). Opinion | The World Is Getting Hacked. Why Don't We Do More to Stop It? *The New York Times*. Retrieved from <https://www.nytimes.com/2017/05/13/opinion/the-world-is-getting-hacked-why-dont-we-do-more-to-stop-it.html>

Tufekci, Z. (2018b, January 20). Opinion | Equifax's Maddening Unaccountability. *The New York Times*. Retrieved from <https://www.nytimes.com/2017/09/11/opinion/equifax-accountability-security.html>

Tufekci, Z. (2018c, January 20). Opinion | Facebook's Ad Scandal Isn't a 'Fail,' It's a Feature. *The New York Times*. Retrieved from <https://www.nytimes.com/2017/09/23/opinion/sunday/facebook-ad-scandal.html>

Tufekci, Z. (2018d, January 20). Opinion | The Looming Digital Meltdown. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/01/06/opinion/looming-digital-meltdown.html>

Tufekci, Z. (2018e, January 20). Opinion | The Truth About the WikiLeaks C.I.A. Cache. *The New York Times*. Retrieved from <https://www.nytimes.com/2017/03/09/opinion/the-truth-about-the-wikileaks-cia-cache.html>

Tufekci, Z. (2018f, January 20). Opinion | Zuckerberg's Preposterous Defense of Facebook. *The*

- New York Times*. Retrieved from  
<https://www.nytimes.com/2017/09/29/opinion/mark-zuckerberg-facebook.html>
- Tufekci, Z. (2018g, April 11). Opinion | We Already Know How to Protect Ourselves From Facebook. *The New York Times*. Retrieved from  
<https://www.nytimes.com/2018/04/09/opinion/zuckerberg-testify-congress.html>
- Tufekci, Z. (2018h, June 8). Opinion | The Latest Data Privacy Debacle. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html>
- Tufekci, Z. (2018i, June 8). Opinion | YouTube, the Great Radicalizer. *The New York Times*. Retrieved from  
<https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html>
- Tufekci, Z. (2018j, July 18). Opinion | What Elon Musk Should Learn From the Thailand Cave Rescue. *The New York Times*. Retrieved from  
<https://www.nytimes.com/2018/07/14/opinion/sunday/elon-musk-thailand-hubris.html>
- Tufekci, Z. (2018k, October 5). Opinion | Russian Meddling Is a Symptom, Not the Disease. *The New York Times*. Retrieved from  
<https://www.nytimes.com/2018/10/03/opinion/midterms-facebook-foreign-meddling.html>
- Tufekci, Z. (2018l, November 5). Opinion | The Election Has Already Been Hacked. *The New York Times*. Retrieved from  
<https://www.nytimes.com/2018/11/03/opinion/midterm-election-hacked.html>
- Tufekci, Z. (2017a, January 27). Opinion | Does a Protest's Size Matter? *The New York Times*. Retrieved from  
<https://www.nytimes.com/2017/01/27/opinion/does-a-protests-size-matter.html>

Tufekci, Z. (2017b, March 9). Opinion | The Truth About the WikiLeaks C.I.A. Cache. *The New York Times*. Retrieved from

<https://www.nytimes.com/2017/03/09/opinion/the-truth-about-the-wikileaks-cia-cache.html>

Tufekci, Z. (2017c, May 13). Opinion | The World Is Getting Hacked. Why Don't We Do More to Stop It? *The New York Times*. Retrieved from

<https://www.nytimes.com/2017/05/13/opinion/the-world-is-getting-hacked-why-dont-we-do-more-to-stop-it.html>

Tufekci, Z. (2017d, September 11). Opinion | Equifax's Maddening Unaccountability. *The New York Times*. Retrieved from

<https://www.nytimes.com/2017/09/11/opinion/equifax-accountability-security.html>

Tufekci, Z. (2017e, September 23). Opinion | Facebook's Ad Scandal Isn't a "Fail," It's a Feature. *The New York Times*. Retrieved from

<https://www.nytimes.com/2017/09/23/opinion/sunday/facebook-ad-scandal.html>

Tufekci, Z. (2016, November 15). Mark Zuckerberg Is in Denial. *The New York Times*. Retrieved from <http://www.nytimes.com/2016/11/15/opinion/mark-zuckerberg-is-in-denial.html>

Tufekci, Z. (2016, November 4). WikiLeaks Isn't Whistleblowing. *The New York Times*.

Retrieved from

<http://www.nytimes.com/2016/11/05/opinion/what-were-missing-while-we-obsess-over-john-podestas-email.html>

Tufekci, Z. (2016, September 12). Did You Hear the Latest About Hillary? *The New York Times*.

Retrieved from

<http://www.nytimes.com/2016/09/13/opinion/campaign-stops/did-you-hear-the-latest-about-hillary.html>

Tufekci, Z. (2016, August 12). The Election Won't Be Rigged. But It Could Be Hacked. *The New York Times*. Retrieved from

<http://www.nytimes.com/2016/08/14/opinion/campaign-stops/the-election-wont-be-rigged-but-it-could-be-hacked.html>

Tufekci, Z. (2016, July 18). How the Internet Saved Turkey's Internet-Hating President. *The New York Times*. Retrieved from

<http://www.nytimes.com/2016/07/20/opinion/how-the-internet-saved-turkeys-internet-hating-president.html>

Tufekci, Z. (2016, May 19). The Real Bias Built In at Facebook. *The New York Times*. Retrieved from <http://www.nytimes.com/2016/05/19/opinion/the-real-bias-built-in-at-facebook.html>

Tufekci, Z. (2016, March 31). Adventures in the Trump Twittersphere. *The New York Times*. Retrieved from

<http://www.nytimes.com/2016/03/31/opinion/campaign-stops/adventures-in-the-trump-twittersphere.html>

Tufekci, Z. (2016, January 1). Why the Post Office Makes America Great. *The New York Times*. Retrieved from

<http://www.nytimes.com/2016/01/03/opinion/why-the-post-office-makes-america-great.htm>

1

Tufekci, Z. (2015, November 20). Stopping WhatsApp Won't Stop Terrorists. *The New York Times*. Retrieved from

<http://www.nytimes.com/2015/11/22/opinion/stopping-whatsapp-wont-stop-terrorists.html>

Tufekci, Z. (2015a, September 23). Volkswagen and the Era of Cheating Software. *The New York Times*. Retrieved from

<http://www.nytimes.com/2015/09/24/opinion/volkswagen-and-the-era-of-cheating-software.html>

Tufekci, Z. (2015a, August 27). "The Virginia Shooter Wanted Fame. Let's Not Give It to Him." *New York Times*. Retrieved from

<http://www.nytimes.com/2015/08/27/opinion/the-virginia-shooter-wanted-fame-lets-not-give-it-to-him.html>

Tufekci, Z. (2015b, August 13). "The Plight of Refugees, the Shame of the World." *New York Times*. Retrieved from

<http://www.nytimes.com/2015/08/14/opinion/zeynep-tufekci-the-plight-of-child-refugees.html>

Tufekci, Z. (2015c, August 10). "Why "Smart" Objects May Be a Dumb Idea." *New York Times*. Retrieved from

<http://www.nytimes.com/2015/08/11/opinion/zeynep-tufekci-why-smart-objects-may-be-a-dumb-idea.html>

Tufekci, Z. (2015d, June 9). "How Hope Returned to Turkey." *New York Times*. Retrieved from

<http://www.nytimes.com/2015/06/10/opinion/how-hope-returned-to-turkey.html>

Tufekci, Z. (2015e, June 4). "Mark Zuckerberg, Let Me Pay for Facebook." *New York Times*. Retrieved from

<http://www.nytimes.com/2015/06/04/opinion/zeynep-tufekci-mark-zuckerberg-let-me-pay-for-facebook.html>

Tufekci, Z. (2015f, April 18). “The Machines Are Coming.” *New York Times*. Retrieved from <http://www.nytimes.com/2015/04/19/opinion/sunday/the-machines-are-coming.html>

Tufekci, Z., & King, B. (2014, December 7). “We Can’t Trust Uber.” *New York Times*. Retrieved from <http://www.nytimes.com/2014/12/08/opinion/we-cant-trust-uber.html>

Tufekci, Z. (2014, March 19). “After the Protests.” *New York Times*. Retrieved from <http://www.nytimes.com/2014/03/20/opinion/after-the-protests.html>

Tufekci, Z. (2012, November 16). “Beware the Big Data Campaign.” *New York Times*. Retrieved from <http://www.nytimes.com/2012/11/17/opinion/beware-the-big-data-campaign.html>

### **MIT Technology Review:**

Tufekci, Z. (2019). How social media took us from Tahrir Square to Donald Trump. (lead story)

<https://www.technologyreview.com/s/611806/how-social-media-took-us-from-tahrir-square-to-donald-trump/>

Tufekci, Z. (2012, June 19). “Data Dystopia: Facebook’s Power Over Our Social Lives Comes with Great Responsibility.” *MIT Technology Review*.

Tufekci, Z. (2011, August 30). “New Media and the People-Powered Uprisings.” *MIT Technology Review*. Retrieved from <http://www.technologyreview.com/view/425280/new-media-and-the-people-powered-uprisings/>

### **Scientific American**

Tufekci, Z. (2019a). Attack of the Zombie Baby Monitors.

<https://doi.org/10.1038/scientificamerican0219-72>

Tufekci, Z. (2019b). More Data Don't Necessarily Help You Make Small Decisions.  
<https://doi.org/10.1038/scientificamerican0319-73>

Tufekci, Z. (2019c). The Real Reason Fans Hate the Last Season of Game of Thrones.  
<https://blogs.scientificamerican.com/observations/the-real-reason-fans-hate-the-last-season-of-game-of-thrones/>

Tufekci, Z. (2019d). Tracking Your Steps and Other Behaviors Isn't Always the Greatest Idea.  
<https://doi.org/10.1038/scientificamerican0519-85>

Tufekci, Z. (2019e). YouTube's Recommendation Algorithm Has a Dark Side.  
<https://doi.org/10.1038/scientificamerican0419-77>

**Wired:**

Tufekci, Z. (2018a). It's the (Democracy-Poisoning) Golden Age of Free Speech | WIRED.  
Cover Story. Retrieved May 21, 2019, from  
<https://www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship/>

Tufekci, Z. (2018b). Why Mark Zuckerberg's 14-Year Apology Tour Hasn't Fixed Facebook |  
WIRED. Retrieved May 21, 2019, from  
<https://www.wired.com/story/why-zuckerberg-15-year-apology-tour-hasnt-fixed-facebook/>

Tufekci, Z. (2018c, December 17). Yes, Big Platforms Could Change Their Business Models.

*Wired*. Retrieved from

<https://www.wired.com/story/big-platforms-could-change-business-models/>

Tufekci, Z. (2019a). What Infowars' Alex Jones and Voldemort Have in Common | WIRED.

Retrieved May 21, 2019, from

<https://www.wired.com/story/infowars-alex-jones-voldemort-platform-attention-gaming/>

Tufekci, Z. (2019b, January 21). Shouldn't We All Have Seamless Micropayments By Now?

*Wired*. Retrieved from

<https://www.wired.com/story/shouldnt-we-all-have-seamless-micropayments-by-now/>

Tufekci, Z. (2019c, February 18). The Imperfect Truth About Finding Facts in a World of

Fakes. *Wired*. Retrieved from

<https://www.wired.com/story/zeynep-tufekci-facts-fake-news-verification/>

Tufekci, Z. (2019d, March 25). Machines Shouldn't Have to Spy On Us to Learn. *Wired*.

Retrieved from

<https://www.wired.com/story/machines-shouldnt-have-to-spy-on-us-to-learn/>

Tufekci, Z. (2019e, April 22). How Recommendation Algorithms Run the World. *Wired*.

Retrieved from

<https://www.wired.com/story/how-recommendation-algorithms-run-the-world/>

Tufekci, Z. (2019f, May 20). We Are Tenants on Our Own Devices. *Wired*. Retrieved from <https://www.wired.com/story/right-to-repair-tenants-on-our-own-devices/>

***Digital Media and Learning Research Hub (MacArthur Foundation):***

Tufekci, Z. (2014, January 9). “Capabilities of Movements and Affordances of Digital Media: Paradoxes of Empowerment.” Retrieved from <http://dmlcentral.net/capabilities-of-movements-and-affordances-of-digital-media-paradoxes-of-empowerment/>

Tufekci, Z. (2013a, October 3). “Pepper Spray and Penguins: Analysis of Turkey’s Social Media-fueled Gezi Protests.” Retrieved from <http://dmlcentral.net/pepper-spray-and-penguins-analysis-of-turkey-s-social-media-fueled-gezi-protests/>

Tufekci, Z. (2013b, July 30). “Anonymity, Internet Surveillance & Lessons from the Anthony Weiner Case.” Retrieved from <http://dmlcentral.net/anonymity-internet-surveillance-lessons-from-the-anthony-weiner-case/>

Tufekci, Z. (2013c, June 20). “Be Quiet and Don’t Move So You Can Be Heard.” Retrieved from <http://dmlcentral.net/be-quiet-and-don-t-move-so-you-can-be-heard/>

Tufekci, Z. (2013d, June 3). “Networked Politics from Tahrir to Taksim: Is there a Social Media-fueled Protest Style?” Retrieved from <http://dmlcentral.net/networked-politics-from-tahrir-to-taksim-is-there-a-social-media-fueled-protest-style/>

***New Yorker:***

Tufekci, Z. (2015, May 15). “Network of Networks.” *New Yorker*. Retrieved from <http://www.newyorker.com/tech/elements/innovation-dial-up-on-the-bosphorus>

### **The Atlantic:**

- Tufekci, Z. (2012a, December 19). "The Media Needs to Stop Inspiring Copycat Murders." Here's How. *Atlantic*. Retrieved from <http://www.theatlantic.com/national/archive/2012/12/the-media-needs-to-stop-inspiring-copycat-murders-heres-how/266439/>
- Tufekci, Z. (2012b, April 25). "Social Media's Small, Positive Role in Human Relationships." *Atlantic*. Retrieved from <http://www.theatlantic.com/technology/archive/2012/04/social-medias-small-positive-role-in-human-relationships/256346/>
- Tufekci, Z. (2011a, March 24). "If We Built a Safer Nuclear Reactor, How Would We Know?" *Atlantic*. Retrieved from <http://www.theatlantic.com/technology/archive/2011/03/if-we-built-a-safer-nuclear-reactor-how-would-we-know/72988/>
- Tufekci, Z. (2011b, January 12). "Delusions Aside, the Net's Potential Is Real." *Atlantic*. Retrieved from <http://www.theatlantic.com/technology/archive/2011/01/delusions-aside-the-nets-potential-is-real/69370/>
- Tufekci, Z. (2010, December 22). "Wikileaks Exposes Internet's Dissent Tax, not Nerd Supremacy." *Atlantic*. Retrieved from [http://www.theatlantic.com/technology/archive/2010/12/wikileaks-exposes-internets-dissent-tax-not-nerd-supremacy/68397/?single\\_page=true](http://www.theatlantic.com/technology/archive/2010/12/wikileaks-exposes-internets-dissent-tax-not-nerd-supremacy/68397/?single_page=true)

### **Financial Times**

- Tufekci, Z. (2015, February 3). "Terror and the Limits of Mass Surveillance." *Financial Times*. Retrieved from

<http://blogs.ft.com/the-exchange/2015/02/03/zeynep-tufekci-terror-and-the-limits-of-mass-surveillance/>

Tufekci, Z. (2014, August 24). "Ban the Executioners of Isis from the Internet's Public Square." *Financial Times*. Retrieved from <http://www.ft.com/intl/cms/s/0/1a3b21e4-2a2b-11e4-8139-00144feabdc0.html#axzz3k8RErN2J>

### **Matter:**

Tufekci, Z. (2014, February 12). "Is The Internet Good or Bad? Yes. : It's time to rethink our nightmares about surveillance." *Matter*. Retrieved from <https://medium.com/message/why-the-great-glitch-of-july-8th-should-scare-you-b791002fff03>

### **Politico:**

Tufekci, Z. (2014, January 4). "Bay of Tweets." *Politico*. Retrieved from <http://www.politico.com/magazine/story/2014/04/cuba-twitter-bay-of-tweets-105382>

### **Nieman Lab (Harvard)**

Tufekci, Z. (2014, December). "The Year We Get Creeped Out by Algorithms." Retrieved from <http://www.niemanlab.org/2014/12/the-year-we-get-creeped-out-by-algorithms/>

### **World Post at Huffington Post**

Tufekci, Z. (2015, March 11). "Facebook Said Its Algorithms Do Help Form Echo Chambers. And the Tech Press Missed It." Retrieved from [http://www.huffingtonpost.com/zeynep-tufekci/facebook-algorithm-echo-chambers\\_b\\_7259916.html](http://www.huffingtonpost.com/zeynep-tufekci/facebook-algorithm-echo-chambers_b_7259916.html)

REPRINTED AT: Tufekci, Z. (2015). "Facebook Said Its Algorithms Do Help Form Echo Chambers, and the Tech Press Missed It." *New Perspectives Quarterly*, 32(3), 9-12.

**The European**

Tufekci, Z. (2013, July 30). "The Limits of Big Data." *The European*. Retrieved from <http://www.theeuropean-magazine.com/zeynep-tufekci--2/7239-the-limits-of-big-data>

"How Social Media Is Changing the Cultural Landscape." (2012, March 1). *The European*.

Retrieved from

<http://www.theeuropean-magazine.com/553-tufekci-zeynep/554-how-social-media-is-changing-the-cultural-landscape>

**The Message:**

Tufekci, Z. (2015a, August 17). “Facebook and the Tyranny of the “Like” in a Difficult World.”

*The Message*. Retrieved from

<https://medium.com/message/how-facebook-s-tyranny-of-the-like-and-engagement-can-be-an-obstacle-to-an-open-and-connected-d4dc03a0d39b>

Tufekci, Z. (2015b, August 1). “Mark Zuckerberg’s Personal News Shows Why Privacy is the

True Bedrock of an “Open and Connected World.” *The Message*. Retrieved from

<https://medium.com/message/mark-zuckerberg-s-personal-news-shows-why-privacy-is-the-bedrock-of-an-open-and-connected-world-e0a1acea89bd>

Tufekci, Z. (2015c, July 31). “The Web of Relationships We Have To Save.” *The Message*.

Retrieved from

<https://medium.com/message/the-web-of-relationships-we-have-to-save-7f337de03e34>

Tufekci, Z. (2015d, July 8). “Why the Great Glitch of July 8th Should Scare You.” *The Message*.

Retrieved from

<https://medium.com/message/why-the-great-glitch-of-july-8th-should-scare-you-b791002fff03>

Tufekci, Z. (2015e, May 7). “How Facebook’s Algorithm Suppresses Content Diversity

(Modestly) and How the Newsfeed Rules Your Clicks.” *The Message*. Retrieved from

<https://medium.com/message/how-facebook-s-algorithm-suppresses-content-diversity-modestly-how-the-newsfeed-rules-the-clicks-b5f8a4bb7bab>

Tufekci, Z. (2015f, April 2). “Where the Danger (Does not) Lurk.” *The Message*. Retrieved from

<https://medium.com/message/germanwings-and-airline-safety-where-the-danger-does-not-lurk-59a4d79d5ef8>

Tufekci, Z. (2015g, March 8). “Make the Most of.” *The Message*. Retrieved from

<https://medium.com/message/make-the-most-of-your-day-351b6e631e0c>

Tufekci, Z. (2015i, January 27). “Ask Not, “Will it Snow?”; ask “What’s the Distribution of

Your Forecast? *The Message*. Retrieved from

<https://medium.com/message/ask-not-will-it-snow-ask-whats-the-distribution-of-your-for-ecast-b7131f5783a9>

Tufekci, Z. (2014a, December 31). "Istanbul's Santa Bear says Merry New Year'smas." *The Message*. Retrieved from

<https://medium.com/message/istanbuls-santa-bear-says-merry-new-years-mas-b74eb22b8b4e>

Tufekci, Z. (2014b, December 1). "How TED (Really) Works: How one hairdresser behind the scenes, and Émile Durkheim, says more about TED than all the viral videos." *The Message*. Retrieved from <https://medium.com/message/why-ted-works-3556066aa9db>

Tufekci, Z. (2014c, November 3). "Hollaback and Why Everyone Needs Better Research Methods." *The Message*. Retrieved from <https://medium.com/message/that-catcalling-video-and-why-research-methods-is-such-an-exciting-topic-really-32223ac9c9e8>

Tufekci, Z. (2014d, October 23). "Ebola: The Real Reason Everyone Should Panic." *The Message*. Retrieved from <https://medium.com/message/ebola-the-real-reason-everyone-should-panic-889f32740e3e>

Tufekci, Z. (2014e, October 17). "What's Wrong with Twitter's Latest Experiment with Broadcasting Favorites." *The Message*. Retrieved from <https://medium.com/message/whats-wrong-with-twitters-latest-experiment-with-broadcasting-favorites-a7c0c81896f7>

Tufekci, Z. (2014f, September 22). "People's Climate March: Can We Scale Up the Politics of Humanity? Failure of Imagination as an Existential Threat." *The Message*. Retrieved from <https://medium.com/message/peoples-climate-march-can-we-scale-up-the-politics-of-humanity-ace57e0985f>

- Tufekci, Z. (2014g, September 4). “Why Twitter Should Not Algorithmically Curate the Timeline: It’s the Human Judgment of the Flock, Not the Lone Bird, That Powers It.” *The Message*. Retrieved from <https://medium.com/message/the-algorithm-giveth-but-it-also-taketh-b7efad92bc1f>
- Tufekci, Z. (2014h, August 14). “What Happens to #Ferguson Affects Ferguson.” *The Message*. Retrieved from <https://medium.com/message/ferguson-is-also-a-net-neutrality-issue-6d2f3db51eb0>
- Tufekci, Z. (2014i, July 22). “Failing the Third Machine Age: When Robots Come for Grandma: Why “caregiver robots” are both inhuman and economically destructive.” *The Message*. Retrieved from <https://medium.com/message/failing-the-third-machine-age-1883e647ba74>
- Tufekci, Z. (2014j, July 9). “Learning From @NateSilver538’s OMG-Wrong #Bra vs #Ger Prediction: Sometimes the Hedgehog Knows a Thing or Two, Problem One: Ignoring Measurement Error in Your Data, Problem Two: Ignoring Field (or Broad) Effects, Problem Three: Humans Are Not Gases in a Chamber, but reflexive beings who react to events.” *The Message*. Retrieved from <https://medium.com/message/learning-from-natesilver538s-omg-wrong-bra-vs-ger-prediction-9d47fa0611e>
- Tufekci, Z. (2014k, June 29). “Facebook and Engineering the Public: It’s not what’s published (or not), but what’s done.” *The Message*. Retrieved from <https://medium.com/message/engineering-the-public-289c91390225>
- Tufekci, Z. (2014l, June 27). “How to Lose 10 Pounds While Playing Dodge-the-Algorithm : Hiding from Facebook meant I couldn’t talk easily to my friends.” *The Message*. Retrieved from <https://medium.com/message/how-to-lose-10-pounds-while-playing-dodge-the-algorithm-88237cd02f95>

- Tufekci, Z. (2014m, May 28). “Expensive Bikes, Cheap Lives: Bait Bikes and Felonies in a Divided San Francisco.” *The Message*. Retrieved from <https://medium.com/message/expensive-bikes-cheap-lives-4b8f66738ba6>
- Tufekci, Z. (2014n, May 15). “The ‘Right to Forget’ a Genocide: The EU Ruling on Google and the Importance of Forgetting.” *The Message*. Retrieved from <https://medium.com/message/the-right-to-forget-a-genocide-4abce84af032>
- Tufekci, Z. (2014o, May 7). “#bringbackourgirls and the Complexities of Attention: Navigating the Power of Attention When It Is Part of What the Cruel Seek.” *The Message*. Retrieved from <https://medium.com/message/bringbackourgirls-and-the-complexities-of-attention-3c3ab5d1dc0e>
- Tufekci, Z. (2014p, April 28). “Forget 140 Characters: Here’s How to Go to Jail for 10 Months for One ‘k;’ Turkey’s Twitter Troubles.” *The Message*. Retrieved from <https://medium.com/message/forget-140-characters-heres-how-to-go-to-jail-for-10-months-for-one-k-ad3d3c5e3c65>
- Tufekci, Z. (2014q, April 22). “What If the Feature Is the Bug? Election monitoring, new power of social media and old power of structural power.” *The Message*. Retrieved from <https://medium.com/message/what-if-the-feature-is-the-bug-7957d8e685c4>

### **Medium (blog posts)**

- Tufekci, Z. (2014a, March 24). “Everyone Is Getting Turkey’s Twitter Block Wrong: Turkey isn’t trying to be North Korea, China or Iran; it’s trying to be Azerbaijan.” *Medium*. Retrieved from <https://medium.com/message/everyone-is-getting-turkeys-twitter-block-wrong-cb596ce5f>

- Tufekci, Z. (2014b, March 21). "The Day the Turkish Government Banned Itself From Twitter: People in Turkey have banned the ban." *Medium*. Retrieved from <https://medium.com/technology-and-society/the-day-the-turkish-government-banned-itself-from-twitter-778b806e38e3>
- Tufekci, Z. (2014c, March 18). "No, Nate, programmers may not be macho, but that's not all there is to it: How French High Theory and Dr. Seuss can help explain Silicon Valley's Gender Blindspots." *Medium*. Retrieved from <https://medium.com/message/no-nate-programmers-may-not-be-macho-but-thats-not-all-there-is-to-it-2f1fe84c5c9b>
- Tufekci, Z. (2014d, February 22). "A Brief Primer on Human Social Networks, or How to Keep \$16 Billion In Your Pocket: 1. Listen to social scientists. 2. Don't reinvent sociology 101. 3. ... 4. Keep \$16 billion in your pocket." *Medium*. Retrieved from <https://medium.com/@zeynep/a-brief-primer-on-human-social-networks-or-how-to-keep-16-billion-in-your-pocket-c290c8ac23dd>
- Tufekci, Z. (2014e, January 13). "Social Media Is a Conversation, Not a Press Release: How @nytkeller and @emmagkeller flunk understanding @adamslisa." *Medium*. Retrieved from <https://medium.com/technology-and-society/social-media-is-a-conversation-not-a-press-release-4d811b45840d>
- Tufekci, Z. (2013a, November 4). "It's a Man's Phone: My female hands meant I couldn't use my Google Nexus to document tear gas misuse." *Medium*. Retrieved from <https://medium.com/technology-and-society/its-a-mans-phone-a26c6bee1b69>
- Tufekci, Z. (2013b, October 29). "The Real Lesson of NSA: If Your Power Depends on Insiders vs. Outsiders, Time for Plan B : And the real scandal is that NSA did not already know this." *Medium*. Retrieved from <https://medium.com/technology-and-society/the-real-lesson-of-nsa-if-your-power-dependson-insiders-vs-outsiders-time-for-plan-b-3aadb5516627>

Tufekci, Z. (2013c, October 2). “Go Ahead, Blame the Internet for DC Shutdown (Hint: It’s Gerrymandering + Filter Bubble): To understand the impact of the Internet, first look to game theory not psychology.” *Medium*. Retrieved from <https://medium.com/technology-and-society/go-ahead-blame-the-internet-for-dc-shutdown-hint-its-gerrymandering-filter-bubble-90d3613bed96>

Tufekci, Z. (2013d, September 6). “If You Argue That the NSA Data Has Not Been Misused, You Must Know Something the NSA Doesn’t: Which isn’t much these days.” *Medium*. Retrieved from <https://medium.com/@zeynep/if-you-argue-that-the-nsa-data-has-not-been-misused-you-must-know-something-the-nsa-doesnt-85a6e531fec4>

Tufekci, Z. (2013e, July 22). “Is the NSA Blinded by Big Data? Who Says It’s the Best Method to Catch the Bad Guys?” *Medium*. Retrieved from <https://medium.com/technology-and-society/is-the-nsa-blinded-by-big-data-e78cbf91290>

7

### **Technosociology (own blog) (Selected posts)**

Tufekci, Z. (2014a, March 11). “A Loaf of Bread, a Dead Child. Turkey’s Protest Cycle.”

Retrieved from <http://technosociology.org/?p=1556>

Tufekci, Z. (2013a, October 11). “Three Cheers to Nobel Peace Prize for not Pandering to

Celebrity Culture.” Retrieved from <http://technosociology.org/?p=1459>

Tufekci, Z. (2013b, June 20). “ ‘Come, Come, Whoever You Are.’ As a Pluralist Movement

Emerges from Gezi Park in Turkey.” Retrieved from <http://technosociology.org/?p=1421>

Tufekci, Z. (2013c, June 12). “What do #occupygezi Protesters Want? My Observations from

Gezi Park.” Retrieved from <http://technosociology.org/?p=1349>

Tufekci, Z. (2013d, June 1). “Is there a Social-Media Fueled Protest Style? An Analysis From

#jan25 to #geziparki.” Retrieved from <http://technosociology.org/?p=1255>

Tufekci, Z. (2012b, November 2). “David Brooks is mistaken, Joe Scarborough is wrong, and

Nate Silver type statistical models are good for democracy.” Retrieved from

<http://technosociology.org/?p=1152>

Tufekci, Z. (2012c, October 14). “Free Speech and Power: From Reddit Creeps to anti-Muslim

Videos, It’s Not \*Just\* “Free Speech.” Retrieved from

<http://technosociology.org/?p=1135>

Tufekci, Z. (2012d, October 8). “Confused by Party ID fluctuations in polls? They Are Probably

Telling Us Something about Confounding Variables.” Retrieved from

<http://technosociology.org/?p=1123>

Tufekci, Z. (2012e, September 17). “Occupy the Political: Politics of Self-Expression and the

Occupy Movement.” Retrieved from <http://technosociology.org/?p=1106>

- Tufekci, Z. (2012f, April 16). "Does Facebook Cause Loneliness? Short answer, No. Why Are We Discussing this? Long Answer Below." Retrieved from <http://technosociology.org/?p=1035>
- Tufekci, Z. (2012g, April 9). "#Egypt's Muslim Brotherhood Teaches a Lesson in Elections in the Age of Twitter and Google Spreadsheets." Retrieved from <http://technosociology.org/?p=1064>
- Tufekci, Z. (2012h, April 9). "What Does Twitter Have to Do With Revolution? (Video of My Talk at Columbia U)." Retrieved from <http://technosociology.org/?p=1021>
- Tufekci, Z. (2012i, March 20). "'We Love You Iranians' campaign on Facebook: War in the Age of Cat Videos." Retrieved from <http://technosociology.org/?p=988>
- Tufekci, Z. (2012j, March 10). "#Kony2012, Understanding Networked Symbolic Action & Why Slacktivism is Conceptually Misleading." Retrieved from <http://technosociology.org/?p=904>
- Tufekci, Z. (2012k, February 20). "The Syrian Uprising will be Live-Streamed: Youtube & The Surveillance Revolution." Retrieved from <http://technosociology.org/?p=832>
- Tufekci, Z. (2012l, February 8). "Breaking Bread, Breaking Digital Dualism." Retrieved from <http://technosociology.org/?p=747>
- Tufekci, Z. (2012m, February 6). "Is the Social Web Less Surprising? The Internet of People and Social Flâneurism." Retrieved from <http://technosociology.org/?p=693>
- Tufekci, Z. (2012n, January 27). "Why Twitter's new policy is helpful for free-speech advocates." Retrieved from <http://technosociology.org/?p=678>
- Tufekci, Z. (2011a, November 30). "Journalism, Social Media and Packs & Cascades: Lessons from an Error." Retrieved from <http://technosociology.org/?p=638>

- Tufekci, Z. (2011b, November 25). "The #freemona Perfect Storm: Dissent and the Networked Public Sphere." Retrieved from <http://technosociology.org/?p=566>
- Tufekci, Z. (2011c, September 19). "Too Many Messages and Only One Facebook Page: April 6th Movement in Post-Mubarak Egypt." Retrieved from <http://technosociology.org/?p=544>
- Tufekci, Z. (2011d, August 30). "Don't Suspend Scout Finch, Mr. Schmidt. It's Wrong and It's Bad for Business." Retrieved from <http://technosociology.org/?p=530>
- Tufekci, Z. (2011e, June 9). "Notes on Amina, Facebook and the Reverse Tragedy of Commons: Pseudonymity under Repressive Conditions." Retrieved from <http://technosociology.org/?p=481>
- Tufekci, Z. (2011f, May 30). "The Revolution Will be Self-Organized, Tahrir, #May27 (part 1)." Retrieved from <http://technosociology.org/?p=448>
- Tufekci, Z. (2011g, May 19). "Why Twitter's Oral Culture Irritates Bill Keller (and why this is an important issue)." Retrieved from <http://technosociology.org/?p=431>
- Tufekci, Z. (2011h, April 13). "Faster is Different. Brief Presentation at Theorizing the Web, 2011." Retrieved from <http://technosociology.org/?p=424>
- Tufekci, Z. (2011i, April 13). "Upcoming Talk: Negotiating Privacy, Boundaries and Visibility in a Networked World: Why We Need to Move Beyond Opt-in vs. Opt-Out." Retrieved from <http://technosociology.org/?p=212>
- Tufekci, Z. (2011j, March 28). "Twitter and the Anti-Playstation Effect on War Coverage." Retrieved from <http://technosociology.org/?p=393>

- Tufekci, Z. (2011k, February 14). "Can "Leaderless Revolutions" Stay Leaderless: Preferential Attachment, Iron Laws and Networks." Retrieved from <http://technosociology.org/?p=366>
- Tufekci, Z. (2011m, February 10). "Let's Mess with Stereotypes: Is Social Media Finally There?" Retrieved from <http://technosociology.org/?p=329>
- Tufekci, Z. (2011n, January 28). "As Egypt Shuts off the Net: Seven Theses on Dictator's Dilemma." Retrieved from <http://technosociology.org/?p=286>
- Tufekci, Z. (2011o, January 15). "Tunisia, Twitter, Aristotle, Social Media and Final and Efficient Causes." Retrieved from <http://technosociology.org/?p=263>
- Tufekci, Z. (2010b, December 9). "Wikileaks is not about secret information; it's about insiders versus outsiders". Retrieved from <http://technosociology.org/?p=220>
- Tufekci, Z. (2010c, October 14). "Wrong Lessons From The Chilean Mine: Technology as the Ultimate Savior." Retrieved from <http://technosociology.org/?p=202>
- Tufekci, Z. (2010e, September 27). What Gladwell Gets Wrong: The Real Problem is Scale Mismatch (Plus, Weak and Strong Ties are Complementary and Supportive). Retrieved from <http://technosociology.org/?p=178>
- Tufekci, Z. (2010f, June 28). "The Unfulfilled Promise of Carr's Shallows (A Long Essay He Thinks You Won't Read)." Retrieved from <http://technosociology.org/?p=151>
- Tufekci, Z. (2010g, May 26). "Facebook, Network Externalities, Regulation." Retrieved from <http://technosociology.org/?p=137>
- Tufekci, Z. (2010h, May 14). "Facebook: The Privatization of our Privates and Life in the Company Town." Retrieved from <http://technosociology.org/?p=131>

Tufekci, Z. (2010i, April 9). “The iPad: The “Jesus Tablet” and the Resurrection of Consumer Society.” Retrieved from <http://technosociology.org/?p=127>

Tufekci, Z. (2010j, March 23). “Who Makes New Friends Online? (Guess again).” Retrieved from <http://technosociology.org/?p=109>

Tufekci, Z. (2010k, February 17). “Google Buzz: The Corporatization of Social Commons.” Retrieved from <http://technosociology.org/?p=102>

Tufekci, Z. (2010l, February 2). “The Consumptive Turn and the Keyboardless Internet: Why the iPad is an Immobilizing Mobile Device.” Retrieved from <http://technosociology.org/?p=86>

Tufekci, Z. (2010n, January 11). “Privacy is a Zombie: Quasi-Public Intimacy and Facebook.” Retrieved from <http://technosociology.org/?p=35>

## **Selected List of News Outlets that have Featured My Work**

### **Newspapers**

New York Times

Washington Post

USA Today

National Post (Canada)

The Guardian

South China Morning Post

### **Broadcast**

Al Jazeera

CNN

MSNBC

National Public Radio

PRI the World (BBC and NPR)

Voice of America (multiple countries)

Radio Free Europe

### **Magazines**

Time

The Economist

The Atlantic

Business Week

Forbes

MIT Sloan Management Review

Le Nouvel Observateur (France's largest weekly newsmagazine)

MIT Technology Review

The European

Science

New Scientist



**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*.

FORM 53

*Courts of Justice Act*

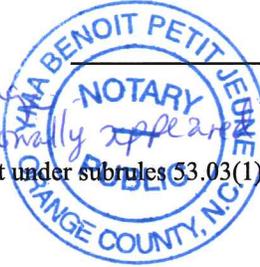
ACKNOWLEDGMENT OF EXPERT'S DUTY

ACKNOWLEDGMENT OF EXPERT'S DUTY

1. My name is Zeynep Tufekci. I live in Chapel Hill, in the state of North Carolina.
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 June 4, 2019

State of N.C., County of Orange  
I certify that Zeynep Tufekci personally appeared



Signature  
\_\_\_\_\_

and signed this document.  
Yma Benoit Petit Jeune  
Notary Public  
Yma Benoit Petit Jeune

NOTE: This form must be attached to any expert report under subrules 53.03(1) or (2) and any opinion evidence provided by an expert witness on a motion or application.

MY COMMISSION EXPIRES: 12/11/2020

RCP-E 53 (July 22, 2014)

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 ZEYNEP TUFEKCI**

**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)**

[ypark@foglers.com](mailto:ypark@foglers.com)  
Tel: 416.365.3727  
Fax: 416.941.8852

**Samantha M. Green (LSO# 63680N)**

[sgreen@foglers.com](mailto:sgreen@foglers.com)  
Tel: 416.860.6904  
Fax: 416.941.8852

**Robert B. Macdonald (LSO# 60512B)**

[rmacdonald@foglers.com](mailto:rmacdonald@foglers.com)  
Tel: 647.729.0754  
Fax: 416.941.8852

Lawyers for the Applicants