Good afternoon, Chair Yang and members of the Commission. First, I would like to thank the Commission for inviting me to this meeting. My name is Ifeoma Ajunwa, I am a Fellow at the Berkman Klein Center at Harvard University and an Assistant Professor at the University of the District of Columbia School of Law. I have authored several papers regarding worker privacy, with an emphasis on health law and genetic discrimination, from which my testimony today is largely drawn.

Today, I will summarize a number of practices that employers have begun to deploy to collect information on employees, and my concerns that such information could ultimately be acquired and sold by data brokers or stored in databanks. There are few legal limitations on how this sensitive information could be used, sold, or otherwise disseminated. Absent careful safeguards, demographic information and sensitive health information and genetic information is at risk for being incorporated in the Big Data analytics technologies that employers are beginning to use -- and which challenge the spirit of antidiscrimination laws such as the Americans with Disabilities Act (the "ADA") and the Genetic Information Non-Discrimination Act ("GINA").

Use of Worker Surveillance Technologies

The technological monitoring of employees by employers is not a new phenomenon. Beginning with punch-card systems, advancing to closed-circuit video cameras, and geo-locating systems, workplace surveillance has become a fact of life for the American worker. What is novel, and of legal concern, is that with technological advancements and lowered costs, employee surveillance now occurs both inside and outside the workplace - affecting the equal access to employment for all Americans.

The potential for worker surveillance now seems limitless. For example, punch clocks have given way to thumb scans, key cards may soon give way to RFID tags, and internet browser histories are often scrutinized. Some employers log keystrokes and many are interested in capturing not only when their employees use private services like Gmail, Facebook, and Twitter, but what they publish there as well. Employer-provided cellphones, an increasingly ubiquitous piece of worker equipment, now offers employers the ability to pinpoint the worker's precise location through GPS. According to a survey from the American Management Association, at least 66 percent of U.S. companies monitor their employees' internet use, 45 percent log keystrokes, and 43 percent track employee emails. Furthermore, many workers may be unaware of the extent to which their employer is tracking them; only two states, Delaware and Connecticut, mandate that employers must inform their employees of electronic tracking.

It is important to note that these new privacy invasions are usually accompanied by the justification that such collection of data serves the employer's business interest of improving efficiency and innovation. For example, one Boston-based analytics firm has developed employee ID badges fitted with microphone, location sensor, and accelerometer and it is testing the badges in 20 companies. The firm claims that it doesn't record conversations or provide employers with individuals' data. Instead, the firm's stated goal is to discover how employee interactions affect the employee's performance. But, the unspoken caveat is that there is no legal barrier to the employer's acquisition of the raw data, which could be used for any purpose, both lawful and unlawful.

In addition to the collection of data through workers' typical workplace activities and movements, some workplaces employ wearable electronic fitness trackers such as Fitbit or Jawbone, often as part of workplace wellness programs. As previous research has shown, the data resulting from fitness trackers is often times irregular.
and unreliable. Furthermore, the data from Fitbits and other such devices require interpretation. Data analytic companies which interpret the data using "industry and public research" are defining the standards that measure a worker's health status and health risks. One problem, as scholars have noted is that medical and health research is rapidly advancing, such that current standards as to what is "healthy" are not the same as they were in the past. Yet, companies that interpret the data from wearables lawfully operate as black boxes, revealing nothing about their data sets and the algorithms used for interpretation.

Another overlooked problem lies in the question of access to the data collected by the employer-provided wearables. Legally, when an employer provides a device for an employee, whether it be a laptop, a mobile phone, or a fitness tracker, that device remains the property of the employer, meaning that the employer could access the data from such devices at any time without permission from the employee. This raises concerns about the privacy of the electronic data collected from employees who use such devices.

A recent trend in worker monitoring is the use of productivity apps. These computer programs, which now represent an $11 billion industry, have been touted as technology that will revolutionize management and that will lead to greater efficiency in the workplace. Even with all the convenience and perceived accuracy that productivity apps could afford human managers, there remains the issue of whether there is an information asymmetry about such apps that negate consent, and whether the invasive nature of such apps could permanently erode worker privacy and provide opportunities for employment discrimination.

As one proponent of the field notes, "today, every e-mail, instant message, phone call, line of written code and mouse-click leaves a digital signal. These patterns can now be inexpensively collected and mined for insights into how people work and communicate, potentially opening doors to more efficiency and innovation within companies." Such discourse, while failing to consider privacy implications, also promotes the ideology that Big Data mined from workers invariably leads to innovation and efficiency gains.

### Increasing Prevalence of Genetic Testing

In addition to workplace surveillance activities conducted by an employer, another area with workplace discrimination implications is the increasing prevalence of genetic testing, and how genetic information could be swept up in Big Data and provide ammunition for employers to engage in genetic discrimination.

The genomics age has brought both scientific advancements in our understanding of how the human genome works and technological advancements allowing for the affordability of genetic testing. Therefore, many more people may discover that they have genetic susceptibility to certain diseases. This in turn increases the likelihood of wrongful disclosure or capture of an individual's genetic information and its misuse for the purposes of employment discrimination. Key Supreme Court cases such as Association for Molecular Pathology v. Myriad Genetics, Inc., which forbids patents on human genes, have further cleared the path to a flood of genetic testing. Already, the number of genetic tests available has grown 72% between 2008 and 2012 (from 1,680 to 2,886 tests). In 2011, the genetic testing market revenue amounted to about $5.9 billion. A recent survey indicates that 81.5% of consumers would have their genome sequenced.

There is now a proliferation of private companies offering genetic testing online. A potential consumer, however, should have ample reason to be wary. In fact, a survey of about 22 genetic testing companies reveals that none of their agreements include a provision regarding the redress of inadvertent disclosures of the information entrusted to their care. It is also of legal concern that recently, a programmer employed one genetic company's open API to create a screening mechanism for websites that works to grant or deny access to a particular website based on a user's genetic make-up (focusing on such factors as race, sex, and ethnic background). Although the genetic testing company quickly moved to block the programmer from using its API, citing its rules against "hate speech," that such a screening mechanism is now possible demonstrates how much more facile technology has made genetic discrimination.

In the digital age, gleaning the genetic information of others has become much easier than most consumers of genetic testing services realize. Going beyond the classic hacking case, in which criminals access sensitive data accompanied by identifying information, even information formerly thought to be anonymous has proven penetrable by third parties. In an article in Science, a group of researchers from the Whitehead Institute of Biomedical Research at M.I.T. demonstrated how they had been able to discover the identities of randomly selected people based on online anonymous genetic information collected as part of a voluntary study. The researchers revealed that they had been able to uncover the identities of individuals within entire families, eventually exposing the identities of nearly fifty people, including relatives who had not taken part in the study. Similarly, other researchers have discovered through their work that RNA expression can be used not only to identify an individual but also to uncover other information about the person, such as weight, diabetic profile, and HIV status. This ease of access to digital genetic information holds dire implications for incidences of genetic discrimination within the employment context.

### Implications For Employment Discrimination

In the age of Big Data, and the "black box" characteristics of its accompanying algorithmic processes, there is legitimate concern that the behaviors, activities, demographic and genetic information of workers collected at the workplace—even if not used directly by the employers collecting it—could become part of datasets that ultimately are used to make employment-related decisions. As so much of the activity behind internet-scraping and machine-learning is not known—nor knowable—-to the people designing the programs, it is not always foreseeable that a certain algorithm will access and deploy prohibited information in its decision-making processes.
My recommendation is that employers should take seriously the worker privacy and employment discrimination concerns raised by big data and worker surveillance, and take steps to minimize the risks posed to their workers.

Thank you for the opportunity to testify today.