IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

MATT DINERSTEIN, individually and on behalf of all others similarly situated, *Plaintiff*, v. GOOGLE, LLC, a Delaware limited liability company, and THE UNIVERSITY OF CHICAGO MEDICAL CENTER, an Illinois not-for-profit corporation, THE UNIVERSITY OF CHICAGO, an Illinois not-for-profit corporation, *Defendants*.	Case No. 1:19-cv-04311 Hon. Rebecca R. Pallmeyer

AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Matt Dinerstein brings this Amended Class Action Complaint and Demand for Jury Trial against Defendant Google, LLC ("Google"), and against Defendants The University of Chicago Medical Center, and The University of Chicago (collectively referred to as the "University" or "University of Chicago"). Plaintiff, individually and on behalf of all others similarly situated, alleges as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. While tech giants have dominated the news over the last few years for repeatedly violating consumers' privacy, Google managed to fly under the radar as it pulled off what is likely the greatest heist of consumer medical records in history. The compromised personal information is not just run-of-the-mill like credit card numbers, usernames and passwords, or even social security numbers, which nowadays seem to be the subject of daily hacks; rather, the personal medical information sold to Google by the University of Chicago is the most sensitive

and intimate information in an individual's life, and its unauthorized disclosure is far more damaging to an individual's privacy.

2. Beginning in or around 2016, Google set in motion a plan to make its most significant play in the healthcare space. This plan had two key components: (1) obtain the Electronic Health Record ("EHR") of nearly *every patient* from the University of Chicago Medical Center from 2009 to 2016; and (2) file a patent for its own proprietary and commercial EHR system that wouldn't be published until well after it had obtained hundreds of thousands of EHRs from the University.

3. EHRs contain patients' highly sensitive and detailed medical records, including records revealing not only a person's height, weight and vital signs, but whether they suffer from diseases like AIDS, cancer, sickle cell, depression, sarcoidosis, or diabetes, or went through a medical procedure like an abortion, transplant, or mastectomy. In short, EHRs are the most personal and sensitive information that exist about a person.

4. The disclosure of EHRs here is even more egregious because the University promised in its patient admission forms that it would *not* disclose patients' records to third parties, like Google, for commercial purposes. Nevertheless, the University did not notify its patients, let alone obtain their express consent, before selling their confidential medical records to Google as part of a research study.

5. In an attempt to provide the public a false sense of security over the legitimate privacy concerns with these practices, Google and the University claimed the medical records were de-identified. But that's incredibly misleading. The records the University provided Google

included detailed datestamps[1] and copious free-text notes. As shown below, Google—as one of the most prolific data mining companies—is uniquely able to determine the identity of almost every medical record the University released.

6. This ability is only increased by and through Google's direct subsidiary, DeepMind, an international leader in artificial intelligence machine learning. In the year following Google's massive medical data grab, it fully absorbed and took control of a division of DeepMind known as "DeepMind Health," for the specific purpose of analyzing medical records and creating commercial products. Google's access to DeepMind's technology allows it to find connections between various data points (*i.e.* from EHRs and Google users' data).

7. Google spent the last decade attempting to gain a foothold in the trillion-dollar per year healthcare industry. But, to develop the type of healthcare technologies most in line with its data analytics and mining platforms, Google needed access to massive amounts of identifiable medical records. To a company like Google—best known for its ubiquitous search engine, but in reality, one of the largest data mining companies in the world—access to that type of data is extremely elusive.

8. To be sure, Google's overtures for such detailed and identifiable records from hospitals, researchers, and healthcare providers alike were all uniformly rebuffed. That is, of course, until Google came across The University of Chicago.

9. The University provided Google a partner willing to turn over the information that it desperately needed. Indeed, the University—seeking not much more than notoriety for its collaboration with Google in the development of healthcare products—was happy to turn over

[1] The term "datestamp," in the medical field, is inclusive of both date and time. Datestamps in the University's electronic medical record system are stored as the number of seconds since midnight on December 31, 1840.

the confidential, highly sensitive and HIPAA-protected records of every patient who walked through its doors between 2009 and 2016. Ultimately, by getting the University to turn over these records, Google quietly pulled off a feat that other tech giants (like Facebook) have had to abandon under mounting public pressure for other gross privacy violations.[2]

10. In exchange for confidential patient medical records, Google agreed to provide the University with a perpetual license to use the software it developed. Other than this limited license, Google kept all intellectual property rights to the software it developed using patients' medical information, including the right to commercialize the software later. To put it another way: Google paid the University for medical information (that rightfully belongs to patients) by providing a license to its proprietary software.

11. The arrangement with the University allowed Google to begin developing software that it can market to hospitals looking improve their bottom lines. Google's product can be sold at premium prices because it targets areas that are very expensive for hospitals: "future healthcare utilization," "emergency department visit[s]," "encounter cost of care," and—critically—"hospital readmission." Readmission in particular is an important matter for hospitals, because Medicare reduces payments to hospitals that have excess readmissions for common conditions such as heart failure or pneumonia.[3] On information and belief, the software Google is developing using Plaintiff's and Class members' private medical information is worth more than $10,000,000.

---

[2] *Facebook sent a doctor on a secret mission to ask hospitals to share patient data*, CNBC, https://www.cnbc.com/2018/04/05/facebook-building-8-explored-data-sharing-agreement-with-hospitals.html?cid=sm_npd_nn_tw_ma (last visited on October 2, 2019).

[3] Centers for Medicare & Medicaid Services, *Hospital Readmissions Reduction Program* (HRRP), https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/Value-Based-Programs/HRRP/Hospital-Readmission-Reduction-Program.html (last visited on October 2, 2019).

12. And as if all of this weren't bad enough, the University also engaged in a cover up to keep the breach out of the public eye so as to avoid the public backlash. The cover up is particularly egregious because the University had a legal duty to inform its patients and the authorities of the unauthorized transfer of their medical records to Google. While this type of public misinformation campaign may be expected from a tech company that has been known to play fast and loose with the information of its customers, the fact that a prominent institution like The University of Chicago would act in such a way is truly stunning.

13. Accordingly, this Complaint seeks all appropriate damages and injunctive relief to address, remedy, and prevent further harm to Plaintiff and the Class resulting from Defendants' gross misconduct.

PARTIES

14. Plaintiff Matt Dinerstein is a natural person and a citizen of the State of Illinois.

15. Defendant Google, LLC, is a limited liability company existing under the laws of the State of Delaware, with its principal place of business located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

16. Defendant The University of Chicago Medical Center is a not-for-profit corporation existing under the laws of the State of Illinois, with its principal place of business located at 5841 South Maryland Avenue, Chicago, Illinois 60637.

17. Defendant The University of Chicago is a not-for-profit corporation existing under the laws of the State of Illinois, with its principal place of business located at 5801 South Ellis Avenue, Chicago, Illinois 60637.[4]

[4] The University of Chicago Medical Center and The University of Chicago are fully integrated entities that have acted jointly in this case. The University of Chicago Medical Center and The University of Chicago are jointly managed and share employees.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.