Report in Brief

June 24, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

A 3-Year Exposure of Privacy Act-Protected Data Revealed USPTO Mismanagement in Safeguarding the Sensitive PII of Trademark Filers

OIG-24-029-I

Background

In June 2023, we learned of the exposure of domicile addresses at the United States Patent and Trademark Office (USPTO) through widespread reporting by the news media. We met with representatives from the Trademarks Organization and USPTO leadership in early August 2023 to gain a better understanding of the incident. We initiated a follow-up review of the actions USPTO took to address the data exposure.

As of December 2023, USPTO managed the registration of more than 3 million trademarks. In recent years, USPTO has detected a rapid increase in potentially fraudulent trademark applications. It has also identified an increase in foreign filings that coincides with the increase in potentially fraudulent trademark applications.

To combat these fraudulent filings, USPTO introduced several safeguards. For example, on August 3, 2019, USPTO implemented the Requirement of U.S. Licensed Attorney for Foreign Trademark Applicants and Registrants, or "the U.S. counsel rule," which requires (1) all filers to provide their domicile address and (2) foreign-domiciled applicants and registrants to have a U.S.-licensed attorney.

Users applying for trademarks provide their personally identifiable information (PII) data—some of which is viewable in the Trademark Status and Document Retrieval (TSDR) system. In February 2023, USPTO determined that domicile addresses in the system had been exposed within publicly accessible web application programming interfaces for 3 years, beginning on February 18, 2020.

Why We Did This Evaluation

Our objective was to assess USPTO's actions in response to the exposure of domicile addresses to determine whether USPTO complied with federal and U.S. Department of Commerce information technology (IT) security standards.

WHAT WE FOUND

USPTO must improve its efforts in safeguarding trademark filers' personal data and sensitive PII. Specifically, we found the following:

I. USPTO mishandled required reporting and notification to affected trademark filers after a 3-year exposure of domicile addresses.

II. USPTO leadership allowed domicile addresses to remain publicly accessible after they were aware of the exposure, risking unauthorized disclosures in violation of the Privacy Act.

III. USPTO did not report that additional sensitive PII was exposed during the incident or notify affected filers that additional data had been exposed.

IV. The Department Chief Privacy Officer did not assist USPTO in responding to the data exposure.

WHAT WE RECOMMEND

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office:

1. Align USPTO policy with departmental requirements to have all USPTO employees report all IT security incidents, including PII exposure, immediately (within 1 hour) once an incident is suspected or confirmed.
2. Establish an internal control process and provide training to ensure all USPTO employees report IT security incidents immediately (within 1 hour) once an incident is suspected or confirmed.
3. Hold USPTO leadership accountable for reporting and notification of IT security incidents in accordance with federal and departmental requirements.
4. Hold USPTO leadership accountable to comply with USPTO risk acceptance policies and procedures.
5. Establish a requirement within USPTO risk acceptance policies and procedures to consider violations of the Privacy Act during IT security incidents.
6. Reassess the non-mission-critical designation of TSDR and other systems supporting the trademark process.
7. Update USPTO policy to meet the federal minimum standard of 2 years and 6 months of log retention.
8. Fully implement log retention controls for USPTO systems according to departmental requirements.
9. Direct the Commissioner for Trademarks to update its applicable System of Records Notice, the *Trademark Manual of Examination Procedure*, and/or its public commitments so that they are all consistent regarding what data will not be publicly viewable.

We recommend that the Deputy Assistant Secretary for Administration:

10. Direct the Office of Privacy and Open Government Director to implement compensating controls and redundant procedures for receiving incidents reported to the Department Chief Privacy Officer.