**<Category of Related Use Cases> – <Infringing a trademark>**

**Goal/Scenario #1**

A corporate employee attempts to prevent misuse of her corporation’s brands and trademarks.

**Brief Format Use Case**

**Use Case:** By various means, both reactive and proactive, persons and/or organization who misuse a trademark online are identified in order to ask them to cease and desist. RDS lookups are the usual initial method for resolving the issue.

**Main Use Case:**

*? Not really sure how this is different from “Use case” and “story”.*

**Casual Format Use Case**

**Title:** A corporate employee attempts to prevent misuse of her corporation’s brands and trademarks in domain names.

**Primary Actor:** A trademark attorney at a company whose trademarks are being infringed.

**Other stakeholders:** Registrant associated with the infringing registered domain name; Registrar associated with the infringing registered domain name; Privacy proxy service engaged by the registrant.

**Scope:** Interacting with RDS; registrant, registrar, other companies being infringed by the same entities, privacy proxy provider, outside counsel.

**Level:** *?*

**Data Elements:** Data elements that allow communication in real or near-real time are the most useful in the context of this use case. These include an email address, an instant messaging address, a telephone number, and/or an indicator that identifies the preferred contact method specified by the Registrant. In cases where the data are incorrect or incomplete, potentially any data element which can be retrieved may be useful for an investigation.

**Main Story:** Terry works in the Legal and Corporate Affairs division of a prominent brand holder corporation. Terry frequently receives information from individual businesses which comprise her company, informing her of sites which violate the trademarks and/or licensing terms of her company in the domain name string or in the content of the site. In fact, this happens several times per week.

Terry also licenses a tool from another party which proactively detects infringements via DNS search, web search, and AI-based analytics.

When infringing sites are identified, Terry uses Reverse WhoIs to identify other sites tied to the registrant. Frequently, the same person or organization is infringing Terry’s company’s trademarks on other sites, or is infringing on the trademarks of other companies.

If the infringing party can be contacted using RDS data, a cease and desist order may be sent. Sometimes a UDRP is filed so that Terry’s company can reclaim the infringing domain. Often, the information is not correct, or is hidden behind a privacy proxy service. In these cases, Terry contacts the registrar, notifies outside counsel, and may resort to additional investigations online to determine the identity of the infringing party.

**Variant story**: Same as above, except that the RDS data falsely identifies Terry’s company as the registrant. In these cases, UDRP is not appropriate. Terry has no recourse except to work directly with the registrar.

**Variant story 2**: Same as above, except that the domain name itself isn’t infringing – it’s the content on the site at that domain name which infringes. (For example, a site at piratesRus.com might be impersonating Terry’s company and using Terry’s company’s trademarks to offer unauthorized software downloads. In these cases, if cease and desist does not change the registrant’s behaviour, Terry must directly ask the registrar to take action. Unfortunately, Terry has only about a 50% success rate with such requests.

**Privacy implications:** Data are collected and stored according to a corporate privacy policy, based on good privacy principles. This privacy policy may be distinct from the public privacy policy Terry’s company publishes regarding the use of customer data and PII.

**Who has control of and access to the data:** The data are collected and stored within a secure system at Terry’s company. This limits the number of employees with access to the RDS data and reduces the risk of the data escaping the company network security boundary. Occasionally data is shared with registries, outside counsel, and law enforcement. Of these, only outside counsel is held accountable to Terry’s company privacy and data handling policy.

**Conditions under which the data are accessible:** These data are available when registrars are in compliance, information is complete and accurate, and privacy proxies are not in use.

**How data can be accessed:** Data are accessed using the various WhoIs implementations of various registrars. Tooling can be created to automate the process and deal with the vagaries of various implementations and protocols.