**Misuse Case:** Doxing is a method of personal intimidation facilitated by the current WHOIS protocol. It involves either an individual or a group of people using the WHOIS service to obtain personally identifiable information on their target, and then posting that information widely across the Internet in the hopes of angering, scaring, or shaming the target. Some reports indicate that [the targets of doxing are most frequently female](https://links8.mixmaxusercontent.com/aMjjKHWxnLSD3SEwj/l/sbVZ44umCZ05PpAZM?messageId=P8yVQkn68kZy5Leov&rn=&re=icmcv5ibuF2YpB0Z31CckBXLzRmct82cudmI). While doxing is not exclusively enabled by WHOIS, it is an instrument frequently misused by attackers and is a tool recommended in a number of doxing handbooks. WHOIS allows the attackers to identify the name, address, and phone number, among other sensitive details, of a domain name registrant in real-time. Armed with this information, the attackers are able to cause emotional, financial, and/or physical harm to the registrant.

**Story:** A person or group of persons accesses the WHOIS protocol to obtain personally-identifiable information associated with a domain name registrant. This process may then be repeated to obtain information about the registrant’s friends or family. The information obtained is used to build a detailed profile of the victim, which is then published online and circulated widely. Attackers vary widely from case to case, but their goal is usually to use a mob mentality to cause real and substantial harm to the victim (with no discernible benefits or gains to the attackers). Some research suggests that victims of online harassment are disproportionally female, non-white, or LGBT. Armed with information sourced through WHOIS, attackers have swatted domain name registrants (swatting is the practice of calling in false tips to law enforcement agencies so that an armed SWAT team is despatched to an address), mailed Qurans to bully those on the basis of their religious beliefs, and even ordered pizzas to be delivered to the address causing embarrassment to the recipient and financial losses to micro enterprises. This is but a small sample of how real people have been victimised as a result of WHOIS as it stands today.

**Data Elements:** *Personally identifiable information?*

In order to prevent misuse by another actor, no personally identifiable information should be stored in the RDS whatsoever. The only data elements the RDS requires to operate are: the domain name itself, the registrar, the domain name’s expiry date, and its status (registered / not registered). For it to be of functional use, there are two optional fields: name servers, and the auth-code.