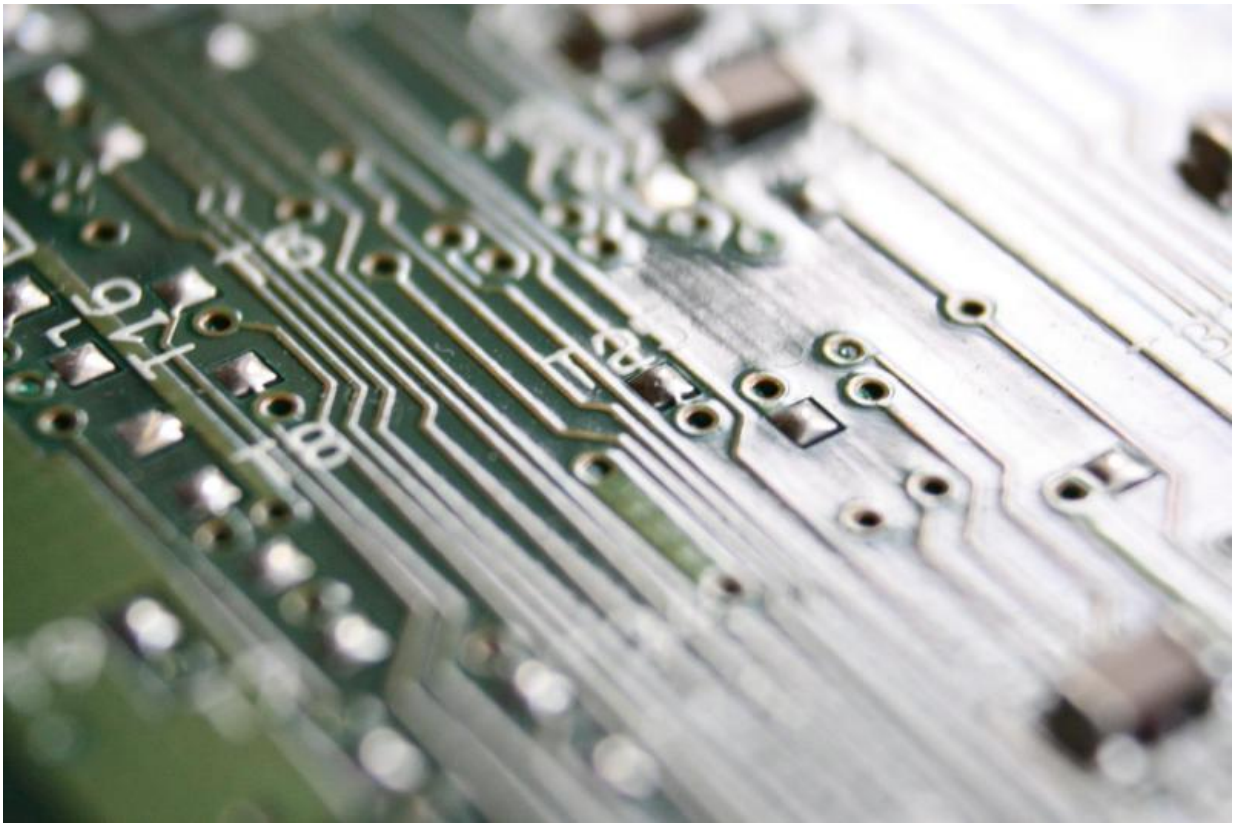
Algorithm protects general privacy in searches by identifying group members to target for closer look

January 12 2016, by Bob Yirka



Credit: Public Domain

(Tech Xplore)—A small team of researchers at the University of Pennsylvania has developed a search algorithm that they claim offers

privacy for protected groups while exposing those sought for a designated purpose. In their paper published in *Proceedings of the National Academy of Sciences*, the team describes the essence of their algorithm, instances in which it might prove useful, and the results they found when running it on publicly available user databases.

Governments around the world have found themselves facing a dilemma since the rise of advanced technology—how to identify terrorists, people with infectious disease, or others, conducting their activities using social media, smart phones or other technology devices, without invading the privacy of everyone else. Recent headlines have suggested that government agencies such as the CIA in the U.S. have resorted to taking a broad approach, tracking everyone, whether they are suspects or not, and monitoring whatever seems to stand out. When such practices became known, the public made it clear that they were strongly against such practices, forcing the government to look for alternatives. In this new effort, the researchers have come up with a search algorithm that they claim offers a way to divide records in a dataset between protected and non-protected individuals, where protected individuals would benefit from "provably privacy-preserving" searching techniques.

The idea behind the algorithm is to use graph searching techniques whereby individuals are prioritized by how close they are to someone else that is a known member of a targeted group. Those that are close to such groups become part of the targeted group, while everyone else has their privacy preserved. It is not a perfect system of course as not everyone that falls close to targeted group members deserves to be targeted—on the other hand, it prevents everyone from having some bit of their privacy breached in the name of national security.

The researchers compared their algorithm against others that seek similar outcomes using the Digital Bibliography and Library Project and the Internet Movie Database and report that the algorithm successfully

identified targeted members without compromising the privacy of those in the non-targeted group, and thus offers an improvement over the all-or-nothing approach. They believe it could prove useful for both governments looking to preserve overall safely, and corporations looking to target only those who might be interested in their products.

More information: Michael Kearns et al. Private algorithms for the protected in social network search, *Proceedings of the National Academy of Sciences* (2016). DOI: 10.1073/pnas.1510612113

Abstract
Motivated by tensions between data privacy for individual citizens and societal priorities such as counterterrorism and the containment of infectious disease, we introduce a computational model that distinguishes between parties for whom privacy is explicitly protected, and those for whom it is not (the targeted subpopulation). The goal is the development of algorithms that can effectively identify and take action upon members of the targeted subpopulation in a way that minimally compromises the privacy of the protected, while simultaneously limiting the expense of distinguishing members of the two groups via costly mechanisms such as surveillance, background checks, or medical testing. Within this framework, we provide provably privacy-preserving algorithms for targeted search in social networks. These algorithms are natural variants of common graph search methods, and ensure privacy for the protected by the careful injection of noise in the prioritization of potential targets. We validate the utility of our algorithms with extensive computational experiments on two large-scale social network datasets.

https://techxplore.com/news/2016-01-algorithm-privacy-group-members-closer.html