When Database Queries are Fourth Amendment Searches

The Fourth Amendment regulates the government's investigative activity by imposing limits on information collection. When that collection qualifies as a "search" or "seizure"—i.e., when it violates a "reasonable expectation of privacy"—the Fourth Amendment normally requires the government to secure a warrant from a neutral magistrate, based on probable cause, that identifies the places to be searched and the things to be seized with particularity. There are two circumstances, however, in which these restraints do not apply—warrant-requirement exceptions and what I call "Fourth Amendment exemptions." In the first set of cases, the government satisfies Fourth Amendment demands merely by demonstrating that the collection was "reasonable." In the second, the collection violates no reasonable expectation of privacy, so the Fourth Amendment simply does not apply. The combination of warrant-requirement exceptions and Fourth Amendment exemptions allows the government to collect an enormous volume of data with no demonstrated connection to crime or specific intelligence needs.

Both courts and commentators have recognized that the scope of the government's collection authority raises significant privacy concerns, the conventional response to which has been to suggest modifications to the Fourth Amendment's regulation of data collection. Collection, however, is only part of the problem. There are also ways to use this voluminous quantum of data that threaten individual privacy. Yet so long as information is collected lawfully, the Fourth Amendment currently has nothing to say about how it is employed.

This Article argues that Fourth Amendment doctrine must do more than heed commentators' calls for collection-focused reform; it must also abandon its laissez-faire approach to the use of information. Reform of collection rules—while important—cannot fully address privacy threats that emanate directly from the use of information. In particular, collection reform cannot eliminate what Professor Daniel Solove calls the "aggregation problem:" By aggregating many bits of information—each of which may come from a different source—the government is able to extract insights that it could not have gleaned from the isolated bits of information alone. In effect, the whole equals more than the sum of its parts. Yet because the Fourth Amendment fails to restrict information use, the government may extract insights from this data free from constitutional constraints.

To address the aggregation problem, I contend that some uses of data aggregation should be considered "searches" subject to constitutional limits. Specifically, this Article focuses on one such tool for extraction: database "queries" about particular U.S. persons. When such queries are reasonably likely to expose knowledge discoverable only by aggregating multiple pieces of data, they can represent an intrusion on individual privacy equally as problematic as any home search or wiretap. They should therefore be recognized as "searches" and regulated accordingly.

This Article will proceed in four parts. Part I will illustrate the breadth and volume of information that the government may lawfully collect. Part II turns to Fourth Amendment doctrine, first explaining how warrant-requirement exceptions and Fourth Amendment exemptions so often render inapplicable the constraints traditionally imposed on searches and seizures, and then exploring the powerful investigative tool this collection authority represents in light of the dearth of Fourth Amendment use restrictions. In Part III, I make the case for treating some queries as searches and explain how the Foreign Intelligence Surveillance Court's (FISC)

jurisprudence regulating government surveillance programs can provide a model for implementing this doctrinal shift. As I have argued elsewhere, the FISC has at times imposed limits on database queries that, while not explicitly based on constitutional foundations, were clearly motivated by Fourth Amendment-related concerns such as individual privacy and freedom from arbitrary government intrusions. In devising a means of imposing on database queries requirements for ex ante review, cause, and particularity in the surveillance context, the FISC has provided a blueprint for what a broader Fourth Amendment use-restriction regime might look like. Part IV then explains why the use restrictions I advocate must be constitutional requirements, rather than simply statutory or regulatory rules. The Article will then briefly conclude.