Guidance for Departments Scanning for SSNs Stored on Servers and Workstations

Some University business and academic processes require the storage of Social Security Numbers, but many campus units continue to store SSNs for processes where they are not explicitly required. In many cases, this is inadvertent and is a result of legacy practices and systems. Security breaches that expose Social Security Numbers pose a significant reputational, financial, and legal risk to our University, so it is in our best interest to limit our potential exposure to these incidents by inventorying and removing SSNs from business processes and systems that do not require them.

The Electronic Communications Policy (ECP) (link is external) protects the privacy of Electronic Communications Records:

"The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations. The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations, while seeking to ensure that University administrative records are accessible for the conduct of the University's business."

Therefore, the following guidelines are provided to assist campus units in inventorying SSNs with tools such as Identity Finder or Spider while still complying with University policy:

Scanning activity must be automated and must be limited to the least perusal of the contents of electronic communications required to accurately inventory high-risk systems for the presence of SSNs, so any scanning program must:

- focus on business systems which are known or likely to contain SSNs and the workstations of those systems' users
- use search expressions written to find SSNs without finding other data, except where that data may be easily misconstrued to be a SSN
- use the same expression(s) consistently across the scan

Balancing the University's goal of conducting an accurate inventory of high-risk systems with the goal of protecting privacy is not always easy, and there is no one-size-fits-all solution; therefore, Table 1 provides policy compliance guidance for departments scanning different types of systems. If after reviewing this guidance, you have questions about whether it is acceptable to scan a particular system, please contact the Privacy Office at privacyoffice@berkeley.edu.

Table 1: Scanning guidance by system type

Type of System	Acceptable to scan?
• Email servers or their database components • Local or cached email folders stored on workstations or laptops	Only with the prior approval of CIO.
• Individual workstations or laptops • Volumes on file or web servers that contain personal data *Examples: User drives or home directories*	Yes, but only with *express consent*[1] from each user.
• Application or web servers, administrative database servers, or volumes on file servers that are reasonably expected to contain no personal data *Examples: Group or departmental file shares, public-facing web servers, database back-ends for business systems*	Yes. Express consent is not required, but notification is recommended as a courtesy to users.

Where it is not logistically feasible to obtain express consent from each user, you must contact the Privacy Office at privacyoffice@berkeley.edu for guidance on developing a scanning program which complies with policy.

For technical questions regarding scanning for SSNs, please contact security@berkeley.edu.

[1]Express consent: Users must be presented with an opportunity to express positive agreement to the scanning, and unless the user takes action to affirm, the department may not assume consent. Express consent is the strongest form of consent, as opposed to negative ("opt-out") or implied consent.