

# What Private Information Google Collects

**Internet Traffic Tracking:** Google is unique in its ubiquitous capability to track the clicks of ~ 99% of Internet users. Google's unique Internet omnipresence results from the near universal adoption of Google's free click-tracking software by websites (Google Analytics & DoubleClick ad-serving analytics), and from 75-90% of Internet users globally using either Google's: search engine, Toolbar, Chrome browser, Android operating system, or tracking "cookies."

- Google's ubiquitous overlapping software capabilities enable Google to track, record, and cross-reference most all click path behavior: i.e. where a user goes, what a user seeks, does, reads or views, how often, and for how long.
- Since Google stores an actual current copy of all of the Internet's trillion plus web pages in its datacenters, when Internet users use a Google search or address bar, they actually are searching Google's database copy of the Internet and not the Internet itself, thus no other entity can track all these click streams.
- Moreover, since Google owns, hosts or aggregates more Internet content on its servers than any entity in the world (YouTube, Google Earth/Maps/StreetView/Books/News/Finance/Blogger/Picassa, etc.), and since Google does not allow competitors to track visits to Google content, Google uniquely tracks these trillions of clicks.

**Email Scanning:** In return for free email services/storage, 175m Gmail users allow their email to be scanned for content so Google can deliver targeted advertising. However, non-Gmail users are unaware that their replies to Gmail and their email address are automatically scanned and stored by Google, and because Google outsources its service to non-Gmail domains, no user could know which of their email replies or email addresses could be scanned/stored by Google.

**Data Collection:** Google sets its default settings to maximize collection of private information.

- Google Buzz' original default setting made users private email lists public when they activated Google Buzz.
- Android's OS default setting keeps tracking users' locations via GPS even when no applications are running.
- Goog-411's default setting allows Google to collect, store and analyze a copy of one's unique voiceprint.
- Chrome browser software automatically downloads and installs updates without notification/permission.
- StreetView's WiFi antennae defaults were set to record all Internet signals/traffic emanating from homes.

Google's default unfettered access to users' computers means if Google is hacked, like in December when its password system computer code was stolen, (NYTimes 4-19-10), the hackers would have unfettered access to users' computers.

## Privacy Record:

- 2003: Google Watch calls Google a "privacy time bomb;"
- 2004: Gmail scans for behavioral advertising; privacy policy changed to allow info- pooling/indefinite storage;
- 2005: Google Earth exposed White House roof security and sensitive U.S. military and foreign installations;
- 2006: Google ignored California privacy law requiring the posting of privacy policy on home page;
- 2007: Privacy International ranked Google worst in world; One World Trust ranked Google "Least Accountable;"
- 2008: StreetView exposed views inside homes, people's faces, & license plates -- many object in many countries;
- 2009: YouTube tracks White House site visitors; Google Books tracks library readers; password security breach;
- 2010: Google to partner with NSA; Google Buzz exposed email lists, Streetview WiFi intercepted Internet traffic.

*Sources: Google; Privacy International; EFF; EPIC; Google Watch; "Googling Security" by Conti; NYT; HitWise; Wikipedia.*

*Fact Sheet by Scott Cleland, President, Precursor LLC, Publisher of [GoogleMonitor.com](http://GoogleMonitor.com) – May 24, 2010*