Governmental Internet Information Collection: Cookies Placing Personal Privacy at Risk

by Norman Gervais

Despite wide concerns about privacy on the Internet and the drastic effects that diminished privacy has, the U.S. government does not have policies that require its own websites to be private. In fact, government agencies use technologies, referred to as cookies, which allow tracking of users on the government’s own websites and even have allowed private companies to track the activities of users on government websites. Former Senator Fred Thompson has expressed unease over this practice, questioning how the government can talk about protecting privacy when it is itself jeopardizing private information [1]. Other people believe that the benefits of these technologies outweigh this cost and provide for a better online experience on government websites [2].

Privacy can be defined as “the right to be left alone” [3, p.127] and may refer to controlling one’s personal information and being free of observation. Privacy is necessary for personal expression, creativity and growth and moreover affects one’s identity [3]. Privacy allows an individual the freedom to control personal information that empowers the regulation of relationships with others and gives people a feeling that they are not objects. If identity were to be treated as an object, individuals would be denied the status of autonomous agents worthy of respect [4].

In today’s digital age, the effect of privacy may be of greater concern than ever. Despite an extensive list of U.S. laws that aim to protect privacy, (see [3], p. 127, for example), advancements in information technology have threatened individual privacy [5] through surveillance and data mining [6]. As Hodson [7, p.24] noted, “EVERY move we make online leaves a trace.”

Although an IP address can provide websites with limited information such as technical specifications on a computer and its general location,
Identity thieves, shopping sites, media companies, advertising companies, charities and even the government are collecting and sharing information about visitors to their websites [14]. Collecting user information is such a common practice that the Wall Street Journal found that almost every commonly visited website was collecting information about user behavior and then selling the data [15]. In addition to a company tracking a user’s movements on the company’s own website, now there are companies specifically termed “tracking companies.” They follow users across the web, collecting information to build profiles on users [16]. Although most of the data are collected to offer a more personal web experience [17], through advertising, for example, there may be future uses and unintended side effects that are not desirable.

Perhaps part of the concern over Internet privacy stems from the fact that a user does not need to give away a lot of personal information to a single entity to have his entire identification revealed. In fact, an individual may be found by marketers, criminals and the government through anonymous data from different sources that are pieced together through a process called re-identification [18]. In addition, the government and civil litigants may seek user information via subpoena. With companies, such as Google, being able to reproduce every search that was made from a specific IP address [19] and Internet providers being able to identify which customer is assigned that IP address [18], individuals may well be concerned about their privacy and who can see what information about them. In addition, even if the government is not using information about website visitors, privacy advocates believe that the government should not record people by using cookies at all [20].

Incentives for Government Use of Cookies

In 2010, the U.S. government updated its online cookie policy. This guidance (M-10-22, Guidance for Online Use of Web Measurement and...
Customization Technologies [21]) updates the previous memorandum (M-00-13, Privacy Policies and Data Collection on Federal Websites [22]) to allow governmental agencies to use third-party websites and applications as well as cookies on their own websites. The goals were to provide a better online experience on government websites, close the IT gap between the private and public sectors, and reach and interact better with a broader audience through social media websites such as Facebook, Twitter and YouTube. At the time of this update, it was unclear if citizens would be comfortable with the use of cookies on government websites [2]. This updated memorandum makes it clear that these tracking technologies can be used. However, the previous guidance did not forbid them either.

Although M-00-13 acknowledged that tracking technologies such as cookies lead to privacy concerns, it did not necessarily ban them. However, it did put forth a process to use them if “…in addition to clear and conspicuous notice, the following conditions are met: a compelling need to gather the data on the site; appropriate and publicly disclosed privacy safeguards for handling of information derived from ‘cookies’; and personal approval by the head of the agency” [22, p.1].

The former need for this strict policy of cookie use may be reflected in the USA.gov guidance that notifies users that in order to minimize access to their information, they need to be aware of their Internet cookie settings [23]. This caution about cookies coupled with their use on government websites may make users question if government websites are safe. Nonetheless, with the 2010 update, it was decided that the process to use cookies should be made easier so that the government could take advantage of the benefits from using them.

As of 2013, both persistent and single-session cookies are being used on government websites. These technologies can now be implemented without personal approval by the head of the agency. They can be used as long as the agency provides a clear notice of the use of such technologies and complies with all other policies, unless multi-session cookies are used with personally identifiable information. These cases require review and approval from the agency’s chief information officer. Also, some governmental services may be made available on third-party websites that have associated third-party cookies (see www.ftc.gov/ftc/cookies.shtm, for example), but the agency should provide an alternative option to the third-party service [21]. In addition, the government is using opt-out cookies (see www.epa.gov/mobilepa/privacy.html, for example), which by default are added to a computer unless the user manually turns them off [24]. The government does, however, provide guidance on how to opt-out if desired (see www.usa.gov/optout-instructions.shtml). In addition to telling a user how not to be tracked with cookies, agencies must post their privacy policies on their websites to allow people to understand agency policies before engaging with them [2].

Resolution of Cookie Use and Privacy

The United States is a democracy, which by definition is a “government by the people” or “a rule of the majority” [25]. Even though the majority of people are not okay with being tracked on the Internet [12] and it poses serious risks to privacy, the government continues to do it. To allow a true democracy, the government should listen to the people and show that it is listening by changing the government’s own policies so that the government itself cannot limit privacy by tracking people on government websites.

The government does, on the other hand, have a responsibility to balance the costs and benefits of any decision that it makes so that the people can overall have the best possible freedom while still having access to an open and transparent government. Since people actually block cookies [13] and actions speak louder than words, one may reasonably assume that people either do not truly care about their information being tracked, believe that the overall benefits of cookies exceed the costs or do not understand how cookies work well enough to block them or make a decision about using them.

These actions, or lack thereof, may advocate for the government’s use of cookies but with limitations that are aimed to protect privacy such as not allowing third-party cookies on government websites. In addition the
government may be able to minimize cookie use by implementing new technologies such as HTML 5’s local storage. This compromise of continued use of cookies, contingent upon government control of user information, combined with keeping current on data security technologies, may not only allow for a better viewing experience on government websites and relieve some of users’ privacy concerns, but also ensure that the information of the users of government websites is under the government’s control so that it will not be misused or used in re-identifying individuals.

Resources Mentioned in the Article

Special Section

Information Policy

GERVAIS, continued

Resources Mentioned in the Article, continued


