Thoughts on General Data Protection Regulation and Online Human Surveillance

By: Nir Kshetri and Jeffrey Voas

Kshetri, Nir and Voas, J. (2020). "Thoughts on General Data Protection Regulation and Online Human Surveillance", IEEE *Computer,* 53(1), 86-90. https://doi.org/10.1109/MC.2019.2951984

Abstract:

The European Union General Data Protection Regulation (GDPR) has introduced online privacy and transparency for consumers as well as legal considerations that companies must address.

Keywords: data protection | legislation | online human surveillance | European Union | GDPR | General Data Protection Regulation | surveillance | privacy | consumer protection | government policies

Article:

The idea of virtually surveilling people poses privacy concerns.[1] Nonetheless, tracking Internet users' online actions in legal, illegal, or extralegal manners is becoming pervasive. For example, data obtained from watching Internet users with cookies and other ways to monitor their online behaviors are useful for marketing and advertising.

The European Union (EU) General Data Protection Regulation (GDPR), which governs personal data in the EU member countries, has dramatically changed the processes that organizations need to follow to track consumers' online behaviors and process that data. Under GDPR, companies are required to obtain specific legal bases to use customers' data and track their behaviors. Many companies choose consent as the option for a legal basis.[11] GDPR requires companies to have an explicit opt-in consent from customers to obtain their personal data.

Key Provisions of GDPR

According to the European Commission, a wide range of items can be considered to be personal data, including information related to an individual's private, professional, or public life. Examples of personal data include names; government identification numbers; physical and email addresses; health, mental, and genetic data; biometric data; racial, cultural, or ethnic information; and data related to online and offline activities, such as location information and Internet Protocol (IP) addresses that allow marketers to track users.[2]

GDPR gives website visitors various rights, which include receiving specific and up-to-date information on the type and purpose of data collected and where the data are sent. Website visitors also have the right to prevent companies from collecting, storing, and processing data regarding them.[12] A company violating GDPR's provisions could be penalized up to 4% of its global annual revenue or €20 million, whichever is greater.[13] This concept is quite novel and somewhat alarming.

Consent may not be needed for cookies that collect "nonsensitive personal data," like those that track items in a shopping cart. However, cookies used to collect personal data tied to users require their consent.

GDPR has certain provisions and principles. Implicit consent was considered to be sufficient to process personal data in the pre-GDPR era. Such consents are implicitly granted by the data subject's actions and the circumstances of a situation (for example, a person's silence or inaction). Under GDPR, data subjects must be informed, in explicit terms, regarding what data will be collected and why. Approaches that do not give users a free choice to say yes or no may be considered to be forced consent under GDPR.[14]

The principle of transparency emphasizes that information addressed to a user needs to be given in clear and plain language: it must be concise, accessible, and easy to understand. In addition, if it is appropriate, visualization must be used. Even after a website has obtained valid consent, visitors should be provided with an easy way to withdraw that consent.[15]

Regulators, such as the U.K. Information Commissioner's Office (ICO) and the French data protection authority, Commission nationale de l'informatique et des libertés (CNIL), have been clear that a cookie notice needs to avoid lengthy, technical details.[16] Another key provision is that entering a website should not require cookie consent. A cookie wall requiring consent to enter or one that does not allow a user to enter without consent is not "freely given" consent.[16]

The attention, so far, has mostly been confined to cookies and other online tracking mechanisms through traditional computers and browsers and users' devices, such as wearables and smart televisions. For instance, the ICO and CNIL have made it clear that the e-Privacy Directive applies to any technique used to read from or write to terminal equipment and also covers device fingerprinting, which is the practice of combining different pieces of information, for instance, operating system, browser, fonts, and clock information, to identify a unique device. However, practical recommendations regarding how firms should obtain informed consent on those devices is lacking.[16]

GDPR may effect the practices of companies that use wearable devices and other methods to monitor employees. For example, a business using fleet tracking will see changes in its right to record data on employees' movements and performance. Employees need to be informed in explicit terms as to what data will be collected and why. GDPR requires legitimate reasons to process employees' personal data. Employers can use the information only for the purpose that had been specified before the data collection, and employees must understand their right to ask for a copy of data in which they can be clearly identified. Such information must be supplied

within 30 days.[17] Likewise, employers need to conduct detailed privacy-impact assessments when they use other mechanisms, such as chip implants, to track their employees.[3]

GDPR Outcomes So Far

As mentioned, consent or the user's approval to process personal data must be freely given, rather than obtained through direct or indirect coercion. The consent process should be unambiguous, transparent, specific, informed, and simple to understand.[18] Many companies' consumer-tracking practices have failed to address several of these major issues and thus lack the legal basis to process personal data. As a result, official complaints against companies have been filed by privacy activists, consumer-protection agencies, and government regulators since the first day GDPR went into effect.[2]

Table 1 presents examples of complaints and formal regulatory actions against U.S. companies that have been initiated by regulators in several EU economies (Table 1). Critics have questioned these companies' legal basis for processing personal data since they lacked mechanisms to obtain the consents that must be "specific, informed and freely given."

Table 1. Examples of complaints filed against U.S. technology companies and the regulatory actions taken.

Company	Complaints	Regulatory actions
Google	Misleading location tracking and web and app activity menus, especially within the Android environment.	The Netherlands, Poland, the Czech Republic, Greece, Norway, and Sweden have filed complaints with their native regulators.[5] France's CNIL fined Google €50 million for violating GDPR, the largest fine so far.[10] Irish DPC investigated Google's ad exchange system, which has 8.4 million websites worldwide, for illegally leaking users' personal data.
Facebook	Criticized for its "take it or leave it" position in consent. Allegedly blocked accounts of users who did not give consent (no free choice).	As of August 2019, 11 cases have been filed against the company in Ireland. In July 2019, the EU Court of Justice ruled that Facebook plugins such as "Like it" in third-party websites violate GDPR.
Twitter	In September 2018, a GDPR complaint was filed with Ireland's DPC, arguing that it exposed users' information to advertisers when they visited a website. The process known as a bid request fails to protect personal data against unauthorized access. In May 2019, a glitch was reported in its iOS app, which enabled the sharing of user location data with an advertising partner.[19]	Irish privacy authorities investigated Twitter regarding its refusal to give users information about how they are tracked when links in tweets are clicked.
Microsoft	Telemetry data collection allegedly collected sensitive data inappropriately, which violates GDPR. It did give users an option to turn the feature off.	In July 2019, German state Hesse banned Office 365 in schools.[20] In July 2019, the Dutch government asked government institutions to avoid Office Online and the Office mobile apps.[21]

DPC: Data Protection Commission

Google

Norway's Consumer Council and other groups have argued that Google lacks a legal basis to track users through location history and web and app activity and then process personal data. These settings are integrated into Google accounts. Complaints have been filed on the grounds that Google's use of the location tracking and web and app activity menus are misleading, especially for users of Android-based smartphones.[4] Even if users turn the location history option off, Google continues to collect location data and tracks consumers through services such as Google Maps, weather updates, and browser searches. To stop the tracking, users need to turn off the web and app activity through settings.[5] Users find it difficult to avoid being surveilled.[22] Plaintiffs argued that Google uses forced consent and thus presses/coerces consumers into consenting to processing data without understanding the details.[4] Critics, in particular, European consumer organizations, have raised important objections to this approach, saying that the setting fails to meet GDPR standards: the relevant information about location history should not be hidden, should not be in submenus, and should not require extra clicks. According to Norway's Data Protection Authority, an additional issue was the lack of clarity regarding how the collected data are used.[6]

In September 2018, French regulator CNIL studied the information that Google makes available for users to create a Google account on an Android phone. Users were presented with much of the information required by GDPR, such as the purposes of data processing, duration of data storage, and categories of personal data. But the consent process it followed was not based on transparency and simplicity to obtain valid consent mechanisms.[23] When new users sign up for an account, they needed to click through a special section to learn about the way Google processes their data. The information is disseminated across multiple documents. To access complementary information, users must click on buttons and links.[4] The CNIL found that, in some cases, as many as five or six actions were needed to access the relevant information. The CNIL also noted that some information lacked clarity and comprehensiveness.[4]

In 2018, a complaint against Google was filed by the chief privacy officer of Brave, a privacy-centric web browser; the Open Rights Group; and University College London. Google's ad exchange system allegedly leaked personal data to more than 1,000 companies without users' consent or their ability to take actions to stop the practice.[24] As of June 2019, the Irish Data Protection Commission (DPC) was investigating this violation.

Microsoft

Concerns have been expressed about Microsoft telemetry data, which is collected from remote/inaccessible points and automatically transmitted to receiving equipment for monitoring purposes. Microsoft allegedly collects data about the use of its Office apps (Word, Excel, and PowerPoint) and records and stores them without informing users. The collected data include sensitive personal information, like email addresses and email subject lines,[20] and requests for translation services through the Office software.[21] Such data are produced by the system-generated event logs.[7] According to a report prepared by the firm Privacy Company, which was commissioned by the Dutch government, Microsoft did not provide users with an option to turn off the feature,[8] which violates a key provision of GDPR.[8]

Twitter

Irish privacy authorities investigated Twitter regarding its refusal to give users information about how they are tracked when links in tweets are clicked. When users put links into tweets, Twitter applies its link-shortening service, t.co, to them. Twitter's stated goals for the link-shortening service is to measure the number of times the link has been clicked. The company argues that such information helps to fight malware. Privacy advocates have argued that Twitter actually gets more detailed information when its users click the shortened links; it is suspected that Twitter might leave cookies in the users' browsers and use the information to track people when they visit other websites.[25]

Facebook

Among other issues, Facebook has been criticized for its "take it or leave it" position regarding consent. It allegedly blocked the accounts of users who did not give consent. If true, this means that there is no free choice, since the only choice for users that do not agree is to delete the account.[14] As of August 2019, the DPC of Ireland (where Facebook's European headquarters are located) had 11 cases against the company.[26] In July 2019, the EU Court of Justice ruled that Facebook plugins, namely, "Like it," in third-party websites that collect and transmit personal data without proper consents violate GDPR.[27]

Violations by others

In terms of the failure to obtain the legal basis to track consumers, U.S. technology companies were not the only violators of GDPR. In February 2019, the Data Protection Authority (DPA) of the German state of Bavaria announced that it studied the website cookie and user-tracking practices of 40 large companies. Many had failed to comply with GDPR, and the DPA was considering imposing fines for their cookie practices. The identified companies were not from the technology industry.[8]

GDPR-Led Changes

In the pre-GDPR era, marketers often tagged users' behaviors with cookies on a hard drive. The regulation treats cookies and other technical identifiers as personal data,[13] meaning that one of the most important requirements of GDPR is that companies must have clear and comprehensive notices regarding cookies. Before GDPR, markets tracked users with IP addresses, which are also treated as sensitive personal data under GDPR. The new regulations give consumers the right to decide whether they want their online behavior to be tracked for analytics and advertising. If companies receive traffic from social media to their websites and use Google Analytics to track visitor behavior, they must get consent.

The GDPR-led changes in virtual human surveillance are drastically changing the business models of marketers and advertisers. As mentioned, noncompliance regulatory fines and penalties have been levied, and marketers and advertisers have pursued diverse tactics and strategies to ensure that they will not face legal sanctions. In May 2018, access to over 1,000 U.S. websites was blocked in Europe.[28]

To comply with GDPR, some websites are removing trackers on websites that serve EU customers. For instance, *USA Today's* European Union Experience does not collect personal information or track or monitor persons visiting from the European Union. This means that it does not deliver a personalized experience to EU customers. The EU version of the company's site has no ads and is faster than the U.S. version. A typical page is about 300 KB compared to 3 MB in the United States.[29]

Consumers do not completely reject organizations' requests for consent to process their personal data. Indeed, a study found that 81% of EU users grant consent to process their data, so that the content and ads they view were personalized.[9] Personal data used by advertisers is almost entirely based on consent.[10]

An important trend is digital advertising, which is returning to the traditional model of contextual advertising that involves displaying ads based on the content a user is looking at in real time, rather than a consumer's static profile. One estimate suggests that this type of ad grew by 15% in one year after GDPR went into effect in May 2018.[10] Advertisers are likely to rely on this information and what is obtained from surveilling users.

The GDPR has brought new challenges to companies that track consumers' online behaviors and use, store, manage, or analyze personal data. With stringent requirements for obtaining consent, GDPR has changed the legal basis regulating surveillance of online behaviors by specifying detailed rules and procedures that are to be followed by companies targeting EU consumers. The regulations have increased the burden on companies since consent to process personal data must be explicit, simple, and easy to understand. GDPR also employs strong penalties for violating its provisions: companies that lacked GDPR-compliant consent for marketing purposes have already faced consequences. GDPR puts new pressures on organizations to modify their marketing and advertising practices with respect to personal data.

References

1. J. Voas and N. Kshetri, "Human tagging," *Computer*, vol. 50, no. 10, pp. 78–85, 2017.
2. J. Jaffe and L. Hautala, "*What the GDPR means for Facebook, the EU and you*," CNet, May, 2018. [Online]. Available: https://www.cnet.com/how-to/what-gdpr-means-for-facebook-google-the-eu-us-and-you/
3. S. Firfiray, "*Microchip implants are threatening workers' rights*," The Conversation, Nov., 2018. [Online]. Available: https://theconversation.com/microchip-implants-are-threatening-workers-rights-107221
4. D. Meyer, "*GDPR: Google hit with €50 million fine by French data protection watchdog*," ZDNet, Jan., 2019. [Online]. Available: https://www.zdnet.com/article/gdpr-google-hit-with-eur50-million-fine-by-french-data-protection-watchdog/
5. C. Merriman, "*Google accused of breaching GDPR with 'misleading' location tracking*," The Inquirer, Nov., 2018. [Online].

Available: https://www.theinquirer.net/inquirer/news/3067108/google-location-tracking-gdpr-breach

6. S. Liao, "*Google still tracks you through the web if you turn off location history*," The Verge, Aug., 2018. [Online]. Available: https://www.theverge.com/2018/8/13/17684660/google-turn-off-location-history-data
7. C. Brook, "*Is Google violating GDPR by tracking EU users*?" Digital Guardian, Dec., 2018. [Online]. Available: https://digitalguardian.com/blog/google-violating-gdpr-tracking-eu-users
8. K. Afifi-Sabet, "*Microsoft under GDPR microscope for Office 365 and OneDrive*," MSN, Nov., 2018. [Online]. Available: https://www.msn.com/en-gb/money/companies/microsoft-under-gdpr-microscope-for-office-365-and-onedrive/ar-BBPKcNs
9. D. Felz, "*Google-style GDPR fines for everyone? Bavarian DPA conducts website cookie practices sweep, announces fines under consideration*," Alston & Bird LLP, Atlanta, GA, Feb., 2019. [Online]. Available: https://www.alstonprivacy.com/google-style-gdpr-fines-for-everyone-bavarian-dpa-conducts-website-cookie-practices-sweep-announces-fines-under-consideration/
10. S. Barry, "*GDPR and advertising: The impact so far*," ADWorld, July, 2019. [Online]. Available: https://www.adworld.ie/2019/07/18/gdpr-and-advertising-the-impact-so-far/
11. D. Meyer, "*GDPR attacks: First Google, Facebook, now activists go after Apple, Amazon, LinkedIn*," ZDNet, May, 2018. [Online]. Available: https://www.zdnet.com/article/gdpr-attacks-first-google-facebook-now-activists-go-after-apple-amazon-linkedin/
12. "*Cookie policy*," Cookiebot. [Online]. Available: https://www.cookiebot.com/en/cookie-policy/
13. A. Onorato, "*Cookies and consent: How GDPR impacts online tracking*," DMNews, May, 2018. [Online]. Available: https://www.dmnews.com/retail/article/13034543/cookies-and-consent-how-gdpr-impacts-online-tracking
14. N. Lomas, "*Facebook, Google face first GDPR complaints over 'forced consent'*," TechCrunch, May, 2018. [Online]. Available: https://techcrunch.com/2018/05/25/facebook-google-face-first-gdpr-complaints-over-forced-consent/
15. K. Lubowika, "*How will GDPR affect your web analytics tracking*?" Piwik Pro, Apr., 2019. [Online]. Available: https://piwik.pro/blog/how-will-gdpr-affect-your-web-analytics-tracking/
16. "*New developments in EU for cookies and online tracking*," National Law Review, Aug., 2019. [Online]. Available: https://www.natlawreview.com/article/new-developments-eu-cookies-and-online-tracking
17. A. Berzinya, "*GDPR's imminent effect on how businesses collect consumers' location data*," Business.com, May, 2018. [Online]. Available: https://www.business.com/articles/gdpr-and-geolocation-data/
18. "*GDPR and advertising: The impact so far*," AdWorld, July, 2019. [Online]. Available: https://www.adworld.ie/2019/07/18/gdpr-and-advertising-the-impact-so-far/

19. J. Stone, "*Real-time bidding, a thriving ad targeting technique, is becoming a GDPR dilemma*," CyberScoop, May, 2019. [Online]. Available: https://tinyurl.com/y63g6gph

20. J. Porter, "*German state bans Office 365 in schools, citing privacy concerns*," The Verge, July, 2019. [Online]. Available: https://www.theverge.com/2019/7/15/20694797/hesse-german-state-gdpr-office-365-schools-illegal-data-protection

21. "*The Netherlands bans Microsoft's mobile Office apps as non-GDPR compliant*," MSPoweruser, July, 2019. [Online]. Available: https://mspoweruser.com/the-netherlands-bans-microsofts-mobile-office-apps-as-non-gdpr-compliant/

22. N. Lomas, "*Google faces GDPR complaint over 'deceptive' location tracking*," TechCrunch, Nov., 2018. [Online]. Available: https://techcrunch.com/2018/11/27/google-faces-gdpr-complaint-over-deceptive-location-tracking/

23. K. Fazzini, "*Europe's huge privacy fines against Marriott and British Airways are a warning for Google and Facebook*," CNBC, July, 2019. [Online]. Available: https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html

24. N. Lindsey, "*Google faces new European investigation over potential GDPR violation*," CPO Magazine, June, 2019. [Online]. Available: https://www.cpomagazine.com/news/google-faces-new-european-investigation-over-potential-gdpr-violation/

25. D. Meyer, "*Twitter under formal investigation for how it tracks users in the GDPR era*," Fortune, Oct., 2018. [Online]. Available: http://fortune.com/2018/10/12/twitter-gdpr-investigation-tco-tracking/

26. E. Price, "*The EU could hit Facebook with billions in fines over privacy violations*," Digital Trends, Aug., 2019. [Online]. Available: https://www.digitaltrends.com/social-media/facebook-gdpr-decision/

27. D. Rankovic, "*EU court rules it's a privacy invasion to have Facebook Like button on websites*," Reclaim the Net, July, 2019. [Online]. Available: https://reclaimthenet.org/eu-facebook-like-button-privacy/

28. J. Davies, "*The impact of GDPR, in 5 charts*," Digiday, Aug., 2018. [Online]. Available: https://digiday.com/media/impact-gdpr-5-charts/

29. J. Scholfield, "*What should I do about all the GDPR pop-ups on websites*?" The Guardian, July, 2018. [Online]. Available: https://www.theguardian.com/technology/askjack/2018/jul/05/what-should-i-do-about-all-the-gdpr-pop-ups-on-websites

Nir Kshetri is a professor of management in the Bryan School of Business and Economics at the University of North Carolina at Greensboro. Contact him at nbkshetr@uncg.edu.

Jeffrey Voas is the editor-in-chief of *Computer*. He is an IEEE Fellow. Contact him at j.voas@ieee.org.