Trackers in Your Inbox: Criticizing Current Email Tracking Practices

Shirin Kalantari, Andreas Put, and Bart De Decker

imec-DistriNet, KU Leuven

Leuven, Belgium

{shirin.kalantari,andreas.put,bart.dedecker}@kuleuven.be

Abstract. Email is among the cornerstones of our online lives. It has evolved from carrying text-only messages to delivering well-designed HTML contents. The uptake of web protocols into email, however, has facilitated the migration of web tracking techniques into email ecosystem. While recent privacy regulations have impacted the web tracking technologies, they have not directly influenced the email tracking techniques. In this short paper, we analyze a corpus of 5216 emails, give an overview of the identified tracking techniques, and argue that the existing email tracking methods do not comply with privacy regulations.

Keywords: Email Tracking · Third Party Tracking · Privacy Regulations.

1 Introduction

Our email inboxes contain traces of most of our online interactions. Today, email delivers messages involving order confirmations, notifications and reminders, social media updates, password recovery links, marketing materials and newsletters, in addition to personal communications. With the persistence of trackers on web traffic, one would also expect the presence of trackers in users' inboxes. In fact it has been suggested that almost 16% of personal conversation emails and 99% of bulk email communications in users' inboxes contain some form of tracking mechanisms [26]. These findings are also confirmed by several academic studies regarding newsletter emails [22,4,3].

In simple terms, email tracking is accomplished by embedding remote resources in an HTML email while making the requests to retrieve these resources identifiable. This simple yet effective strategy is becoming increasingly pervasive to the extent that it has been proposed by several online tracking businesses as “*the solution for cookie-less tracking across devices*” [21,5,11].

Email tracking often involves third parties who receive fine grained, personal information about the recipients such as the newsletters they are subscribed to, online services they are using, their email reading habits, and potentially even IP addresses. This information might be valuable to spammers for *personalizing* their phishing and spamming attacks, as including personalized context in phishing attacks amplifies their impacts. For example, the *Emotent* phishing campaigns,

identified as one of the “*top malware threats affecting Europe*” [12], employed such techniques. Furthermore, there are businesses interested in sneaking into users’ inboxes to gain business insights from their bulk emails. In 2017 *Unroll.me*, a free service that allows users to manage their newsletter subscriptions, sold parts of its users’ data to Uber [16].

While recent studies suggest that many of the technologies employed in web tracking are impacted by new privacy regulations [7,20], there has been little academic activity concerned with investigating whether the existing email tracking techniques abide with these regulations. Therefore, our study aims to initiating a debate on the compliance of current bulk email communication tracking methods with existing privacy regulations. For this purpose we analyzed the newsletter emails of 142 websites and evaluated their email tracking techniques, answering the basic questions: which data is actually being collected, by whom, and for which purposes?

2 Background

This section contains an overview of the main entities in bulk email communications and background information on HTTP emails and HTTP requests. The term ‘bulk email’ refers to non-conversational emails that target a broad range of recipients such as newsletters, marketing campaigns and order confirmation.

2.1 Main Entities

The main entities that drive bulk email communications are:

Campaign owners: These are the businesses that employ email communication to reach their audience.

End users: The end users, or email recipients, either explicitly subscribe to newsletters or receive bulk emails as part of the services they are using (e.g., social media updates, online purchase confirmation, reminders, etc.). Users access their email through *Email Clients*, also called Mail User Agents (MUAs). MUAs can be categorized into two major types: web clients like Gmail, and local mail clients like Thunderbird and iOS Mail.

Third Party: The campaign owner might want to include a number of third parties into their campaign emails. For example they might integrate advertisement partners such as Facebook or Instagram Ads, email optimization services such as mailing list sanitation tool *ZeroBounce*¹ or subject line personalization service *phrasee*, and/or marketing platforms such as *Salesforce*² or *Google Analytics*³.

¹ <https://www.zerobounce.net/>

² <https://www.salesforce.com/>

³ <https://analytics.withgoogle.com/>

Email Service Providers (ESPs): Campaign owners often outsource the actual email process to an ESP. This entity manages the mailing list, provides email templates, and most importantly sends out the campaign emails. Examples of well-known ESPs include Mailchimp, Selligent, and Campaign Monitor. In addition, an ESP provides integration tools, allowing marketers to seamlessly integrate third parties into their marketing platform.

Mailbox providers: Each email address is registered with a mailbox provider. It offers email hosting for users to send, receive and store their email messages. Gmail and Yahoo! are examples of widely used mailbox providers. Additionally, mailbox providers offer email security services such as spam filtering, malware detection, and transport layer encryption to protect users from malicious content.

2.2 HTML Emails

Despite supporting styling and rich text formatting, HTML emails have been criticized for their security and privacy issues since their inception [29,6,30,25]. First of all, certain HTML tags could be exploited in the context of email. For instance, including malicious code within a `<script>` tag in an HTML email could allow for wiretapping email communications [31]. Secondly, interacting with certain HTML elements embedded in the email can result in the execution of a series of HTTP requests that include detailed information about the recipient. These requests are made by the email client in order to load the remote resources included within HTML emails.

Partial countermeasures have been adapted to minimize the scope of these two issues of HTML emails. Some HTML tags are removed by the email clients before rendering the email. However, there is no standard that defines *safe* HTML tags. Therefore, it is left to email clients to decide which elements to remove from an HTML email. For example, some email clients even execute scripts within HTML emails [27].

An important advantage of HTML emails is the possibility to embed remote resources such as hyperlinks and images. Together, these two types account for 98% of all remote resources in newsletter emails [17]. However, HTML emails introduce new threats to the user's privacy, as it allows to embed identifiable information in the requests made by the email client. This problem can be quite severe as these requests are made as soon as the email client renders the HTML email.

As a countermeasure, email clients block remote resources either by default or through user settings. While this stops the HTTP-based tracking, it negatively impacts user experience and provides no protection once the user decides to load remote contents. Despite the shortcoming of current countermeasures in resolving privacy and security issues of HTML emails, they are still the de facto choice for receiving newsletter emails.

2.3 HTTP requests

When clicking on a URL or loading a remote resource, the email client executes an HTTP request. This request can be represented as follows:

GET request-URL [request-header]*

In this representation *GET* identifies the type of request. GET requests are the most common type of HTTP requests, and are used to request data from a specified resource or webserver. Next, the *request-URL* represents the address of the remote resource. In newsletter emails, senders often embed personalized tracking tokens in the *request-URL* [9,22,15,17]. Such a tracking token could be any string that maps to the recipient email address, or identity, at the server side. Personalized URL tokens have been used in email for more than 20 years [29], and they are still pervasively used in newsletter emails [22,17,15]. From a technical perspective personalized URL tokens can be seen as cookies included in the URL instead of HTTP headers. This technique has recently gained traction in web as a form of cookie-less tracking [8]. Finally, the *request-header* consists out of one or more HTTP headers. These headers are attached by the email client to the request in order to help the webserver that serves the remote resource in providing a tailored response.

After a client executes an HTTP request, the webserver will return an *HTTP response* of the following form:

Status-code [response-header]*

Webservers use these status-codes to briefly convey information to clients about the status of their request. Two of the most well known status-codes are: 200 OK (the request was successful) and 404 Not Found (the server cannot find the requested resource). Other status-codes indicate that the client needs to execute further steps. For example, redirect responses (ranging from 300 to 308) indicate that the client needs to get the requested resource using another URL. Redirect chains have been used for tracking purposes by involving third parties before serving a resource [9,10,1]. The *response-header* consists out of one or more HTTP headers that allow the server to pass additional information about the response. For example, the response header *Set-Cookie* is used to set a cookie on the email client and *Cache-Control* header specifies the caching policy for the requested resource informing the email client how to deal with subsequent requests for the same resource; whether to load it from cache storage or whether to make a fresh HTTP request.

3 Related work

In academic literature, email tracking has been viewed as the consequence of loading remote resources in HTML emails. Bender et al. [3] identified that senders do adapt their sending behavior according to the information conveyed through email tracking. For instance, they send fewer emails to less engaged inboxes and

personalize the email content based on the device that the recipient uses for opening their emails (e.g. iPhone users receive more contents related to Apple products).

Based on the assumption that tracking and functional contents are separable, Fabian et al. [13] gathered a corpus of newsletter emails and identified a number of features for tracking images. The email corpus and the detection method were extended in [4] and [15]. These identification techniques aim to improve the content blocking, by allowing non-tracking and functional contents to load.

Englehardt et al. [9] found that loading remote contents in an email can leak the recipient’s email address to third parties by analyzing a large scale corpus of commercial newsletters. Xu et al. [32] illustrated the feasibility of email tracking for launching a long-term surveillance attack against the recipients. They also conducted a user study and concluded that the majority of participants were unaware of the privacy risks of email tracking.

Maass et al. [22] developed PrivacyMail⁴, an email transparency platform that reports a privacy score and an elaborate analysis of email tracking practices for each newsletter. In [17] the author discussed the privacy risks of email tracking for obtaining read receipts and discussed the shortcomings of existing countermeasures.

4 Methodology and datasets

This section give an overview of the dataset that was used and the analysis performed on it.

Dataset: Two main approaches are used in literature to assemble a corpus of mailing-list/newsletter emails: manual and automated approaches. In the manual approach, applied by [22,3,15], a human searches a website for a newsletter subscription form and signs up email addresses. In the automated approach, as used in [17,9], an automated crawler will analyse web-pages in search for newsletter subscription forms. Next, the crawler attempts to sign up email addresses to the subscription without user interaction. While this offers obvious benefits, it has two important shortcomings for our use-case. Firstly, the automated approach needs adaptation for use in multi-language contexts, such as EU-based newsletters, in order to detect the subscription form. Secondly, its performance decreases when it is used for subscribing multiple identities to a newsletter, due to the non-deterministic nature of most crawlers. Thus, we decided for a corpus with manual subscription in which multiple identities are subscribed to each newsletter. In addition, we included the corpus collected by Maas et al. [22] in PrivacyMail.

Email preprocessing: A preprocessing step was performed on each email object in the corpus. First, the HTML was extracted from the email body. From the HTML code, the URLs of hyperlinks and images were extracted. We also checked whether the HTML emails contain embedded images using Content-ID or data

---

⁴ <https://privacymail.info/>

URI schemes [24]. Both the **List-Unsubscribe** header and the unsubscribe link within the HTML part were used to determine whether opt-out options are provided. To find the unsubscribe link, the method used in [17] was adapted with additional unsubscribe keywords in French, German and Dutch.

Identifying third parties: We define the first party as the domain name of the website to which the user was subscribed, its sub-domains and possibly a related but different top-level domain (e.g. we considered `urbandecay.com` a first party to `urbandecay.co.uk`). Consequently, third parties are any other domains different than the first party domains.

To find third parties included in an email we used a static and a dynamic search. In the static approach we performed a text search in the email body for the domain names used in the sender’s email address (e.g. `example.com` in `info@example.com`) and the URLs of remote resources (i.e. links and images). In the dynamic search, we looked for third parties in the redirect chain of the HTTP request for loading remote images. However, the remote resources in older emails are often deactivated, causing the HTTP request to return an error code. Therefore, only emails sent at most one month prior to this study are considered, as the SPAM-ACT requires opt-out options to stay at least 30 days functional after an email is sent [14]. On the first attempt we loaded images in 5216 emails, from 142 senders between the period of 2020-03-23 to 2020-04-23.

Regarding the information that each third party could receive via emails, third parties that are included through the email address receive the email address of the recipients, other third parties that are included through the HTTP requests might set cookies on the user’s device and receive the personalized tokens that are included in the request URL. Moreover, since HTTP depends on transport layer protocols, these third parties also receive metadata such as the IP address and the user agent of the recipient. For identifying personalized URL tokens, we used the differential method used in [22,15,3,17], and compared the structure of request URL in emails sent to multiple users.

5 Result

While our analysis is ongoing, our initial results provide insights into privacy hazards of email tracking.

General findings: All the 5216 emails in the analyzed corpus are HTML-enabled. This shows the uptake of HTML emails in recent years since Bender et al. [4] detected 72% of emails in their newsletter corpus as HTML in 2016. For the majority of emails we were able to find an opt-out option: 89% of emails included the *List-Unsubscribe* header and for approximately 93% of emails we were able to find an unsubscribe link. Our dataset confirms the popularity of remote images and links in email as 90% of emails included more than 8 remote images and 11 links. On the other hand embedded images are rarely used as only 3 senders used embedded images inside their emails. In one email the image was embedded using the data URI scheme and the rest used *Content-ID* scheme.

Third parties in email: In the analyzed corpus, 89% of the emails embed resources from at least one third party with a mean and median of two per email. Figure 1 indicates the number of third parties that senders include in their newsletter emails. In total, 12 senders use a third party domain in the email address that they used for sending their newsletter emails. The majority of third parties are included through HTTP requests. In 1619 emails (31% of the total emails) from 29 senders, new third parties are included through the redirect chain of HTTP requests for loading images. Regarding the information that third parties receive, 62 senders allow third parties cookies to be set on recipients’ devices and the majority receive personalized URL tokens. Also note that every HTTP request leaks TCP/IP metadata such as IP address and timezone. Table 1 summarizes the top third parties in our corpus and the type of information that they receive.

Table 1. The most common third parties by number of sender. *Aggregated result for different domains.

Third party	Information received	Number of senders
Mailchimp*	metadata, URL token, cookie	26
Klaviyo*	metadata, URL token	22
shopify.com	metadata, URL token	15
amazonaws.com	metadata, URL token	12
returnpath.net	metadata, URL token	11
Google*	metadata, URL token	10

Fig. 1. Third party distribution per sender.

Next, the caching policy of remote images in emails has been analyzed. Interestingly, we noticed that in emails of 90 senders (64% of all senders) either a no cache or a short cache policy of maximum 2 hours is used for remote images. Thus, these senders and the third parties they include in their emails receive fresh HTTP requests potentially every time the recipients open these emails.

6 Discussion

Our results mainly confirm the findings of previous studies: email tracking is very common and it leaks information to third parties. However, the main goal of this study is to initiate a debate on the compliance of current email tracking practices with privacy regulations. We also want to call for collaboration between legal and technical communities since mitigating the privacy risks of email tracking requires a mutual effort.

An interdisciplinary effort is required to fully investigate the compliance of mass email communication. We illustrate the importance of this effort by indicating a shortcoming in the existing technical approaches. The third party analysis is performed in this paper and many of the previous related works only provide a partial view on the email tracking ecosystem. This analysis is based on the assumption that a third party service uses a different domain name than the sender. While trivial at first, this assumption does not always hold: a tracker can control a subdomain of the first party, through DNS CNAME setting. Dimova et al. [8] recently conducted a large-scale analysis of CNAME tracking in web, detecting it in almost 10% of top 10K websites. Although such large-scale analysis is missing for email datasets, CNAME trackers has been identified in newsletter emails. Kalantari [17] found an example of a CNAME tracker which uses the sender domain to serve advertisement in newsletter emails and bypass the privacy protection block lists. Similarly, we find two ESPs that perform tracking while hiding under the sender domain. The ESP Klaviyo⁵, deploys CNAME tracking to control a subdomain of the sender [18]. The other ESP, Selligent⁶, appears to track users by requiring their software to be installed on the first-party webserver. This software will then process HTTP requests with a specific URL structure. We find the URL structure of Selligent in 1159 emails (that is 22% of all emails) in our corpus.⁷

While a full legal assessment of email tracking is left as a future work, in the remainder of this section we criticise two common misconceptions about the legitimacy of email tracking.

⁵ <https://www.klaviyo.com/>

⁶ <https://www.selligent.com>

⁷ The URL structure was detected based on the answer provided in Stackoverflow at <https://stackoverflow.com/questions/33002037/which-email-software-is-used-optiext-optiextension-dll-in-url>

6.1 Email tracking far beyond a legitimate interest

Senders may argue that email tracking is lawful since it measures the effectiveness of the email marketing strategy. However, for this processing to be lawful, a balance between information minimization and transparency must be maintained. First of all, by making the HTTP requests in email individually identifiable, senders can measure far more than the “overall performance” of their campaign. It enables them to individually identify recipients that interacted with their emails and the devices they used among other information. Furthermore, as our results illustrate the majority of senders specify a short cache period for remote resources in their email which enables them to receive these information *every time* the recipient interact with these emails.

Finally, email tracking could only be considered legitimate if senders fulfill their information obligation toward recipients. They might use email tracking to offer optimized or tailored services to their recipients. For example, many ESPs offer send time optimization services [28,23,19] to deliver emails according to the recipients email reading habits. Similarly, Bender et al. [3] noticed that the content of newsletter campaigns are adjusted based on the email client that the recipient uses for reading previous emails (i.e. iPhone users receive more contents related to Apple products). However, we believe that an explicit user consent should be obtained for service personalization and the subscribed users should be able to opt-out from personalized tracking while still receiving the non-personalized newsletters.

6.2 Email tracking far beyond a data protection interest

Some senders might argue that email tracking can be used to protect the privacy of recipients as they stop sending emails after a certain period of recipient inactivity (e.g. one year). In fact, when Bender et al. [3] exhibited different email reading behavior for email addresses subscribed to the same newsletters, they noticed a significant difference in the campaigns’ sending rates: the less engaged inbox started receiving emails at a lower frequency.

However, adapting sending rates mostly serves the interest of sender: it prevents frustrated users from unsubscribing from their mailing-list or reporting their emails as spam, which jeopardizes their reputation and delivery rate. It should be noted that for users the consequences of unsubscribing from a newsletter is different than receiving fewer emails. Unsubscribing from email communications often entails legal obligations that protects the recipient for example by mandating the erasure of user’s data.

7 Conclusion

Although email tracking is performed by hackneyed techniques and despite the awareness of academic community about its consequences, there has been little interest in evaluating email tracking from the eyes of privacy regulations.

However, it should be noted that *“Many perverse aspects of information security that had been long known to practitioners but just dismissed as ‘bad weather’ have turned out to be quite explicable in terms of the incentives facing individuals and organisations”* [2].

Email privacy guidelines have not been adapted as the email ecosystem has evolved and they do not protect users against the current methods of email tracking. Email technologies on the other hand are advancing at a rapid pace. Gmail recently enabled Accelerated Mobile Pages (AMP) for newsletter emails, which allow recipients to directly make transactions from their emails⁸. To overcome the risks of email tracking a collaboration between legal experts and technical scholars is needed to formalize technically sound guidelines based on existing privacy regulations.

Acknowledgments We would like to thank Pierre Dewitte for his insightful comments during the early stages of this research, as well as Max Maass and PrivacyMail (<https://privacymail.info/>) for their willingness to share data related to this study.

References

1. Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., Diaz, C.: The web never forgets: Persistent tracking mechanisms in the wild. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 674–689. CCS ’14, ACM (2014). <https://doi.org/10.1145/2660267.2660347>
2. Anderson, R., Moore, T.: The economics of information security. *Science* **314**, 610 (11 2006). <https://doi.org/10.1126/science.1130992>
3. Bender, B., Fabian, B., Haupt, J., Lessmann, S., Neumann, T., Thim, C.: Track and treat - usage of e-mail tracking for newsletter individualization. In: Twenty-Sixth European Conference on Information Systems (ECIS2018), Portsmouth, UK, 2018 (06 2018)
4. Bender, B., Fabian, B., Lessmann, S., Haupt, J.: E-mail tracking: Status quo and novel countermeasures. In: Proceedings of the thirty-seventh international conference on information systems (ICIS). Dublin, Ireland 2016 (12 2016)
5. Conversant: Five building blocks of identity management. https://www.conversantmedia.com/hubfs/US%20Conversant/IMAGE%20ILLUSTRATIONS%20and%20VIDEOS/Resource-center-assets/PDFs/Five_Keys_to_Identity_Resolution_24Apr2019.pdf, last accessed on 2020-12-15
6. Coursen, S.: Solving the problem of html mail. <https://www.securityfocus.com/columnists/58>, last accessed on 2021-02-02 (2002)
7. Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., Weippl, E.: Measuring cookies and web privacy in a post-gdpr world. In: Choffnes, D., Barcellos, M. (eds.) *Passive and Active Measurement*. pp. 258–270. Springer International Publishing, Cham (2019)
8. Dimova, Y., Acar, G., Olejnik, L., Joosen, W., Van Goethem, T.: The cname of the game: Large-scale analysis of dns-based tracking evasion. *Proceedings on Privacy Enhancing Technologies* (2021), <https://arxiv.org/pdf/2102.09301>

⁸ <https://amp.dev/about/email/>

9. Englehardt, S., Han, J., Narayanan, A.: I never signed up for this! privacy implications of email tracking. *Proceedings on Privacy Enhancing Technologies* **2018**(1), 109–126 (2018)
10. Englehardt, S., Narayanan, A.: Online tracking: A 1-million-site measurement and analysis. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. pp. 1388–1401. CCS '16 (2016). <https://doi.org/10.1145/2976749.2978313>, <http://doi.acm.org/10.1145/2976749.2978313>
11. Epsilon: The way the cookie data crumbles: People-based profiles vs. cookie-based solutions. <https://www.epsilon.com/hubfs/Cookie%20Crumbles.pdf>, last accessed on 2020-12-15 (2019)
12. Europol: Internet Organised Crime Threat Assessment (IOCTA) 2020. European Union Agency for Law Enforcement Cooperation (Europol) (2020)
13. Fabian, B., Bender, B., Weimann, L.: E-mail tracking in online marketing - methods, detection, and usage. In: *12th International Conference on Wirtschaftsinformatik* (March 2015)
14. FTC.gov: Can-spam act: A compliance guide for business. URL: <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business>, last checked on 2021-02-17
15. Haupt, J., Bender, B., Fabian, B., Lessmann, S.: Robust identification of email tracking: A machine learning approach. *European Journal of Operational Research* **271**(1), 341 – 356 (2018). <https://doi.org/10.1016/j.ejor.2018.05.018>
16. Isaac, M., Lohr, S.: Unroll.me service faces backlash over a widespread practice: Selling user data. <https://nyti.ms/2pYH0Eb>, last accessed on 2020-12-15 (2017)
17. Kalantari, S.: Open about open rate? In: *IFIP International Summer School on Privacy and Identity Management*. p. (to appear). Springer, Cham (2021)
18. Klaviyo Help Center: How to set up dedicated click tracking. URL: <https://help.klaviyo.com/hc/en-us/articles/360001550572-Setting-Up-Dedicated-Click-Tracking>, last checked on 2021-02-20
19. Klaviyo Help Center: Smart send time in klaviyo. <https://help.klaviyo.com/hc/en-us/articles/360029794371-Smart-Send-Time-in-Klaviyo>, last accessed on 2021-02-21 (2021)
20. Lefrere, V., Warberg, L., Cheyre, C., Marotta, V., Acquisti, A.: The impact of the gdpr on content providers. In: *The 2020 Workshop on the Economics of Information Security* (2020), <https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final43.pdf>
21. LiveIntent: Overview of custom audiences. <https://support.liveintent.com/hc/en-us/articles/204889644-Overview-of-Custom-Audiences>, last accessed on 2020-12-15 (2020)
22. Maass, M., Schwär, S., Hollick, M.: Towards transparency in email tracking. In: Naldi, M., Italiano, G.F., Rannenber, K., Medina, M., Bourka, A. (eds.) *Privacy Technologies and Policy*. pp. 18–27. Springer International Publishing, Cham (2019)
23. MailChimp: Insights from mailchimp’s send time optimization system. <https://mailchimp.com/resources/insights-from-mailchimps-send-time-optimization-system/>, last accessed on 2021-02-20 (2014)
24. Masinter, L.: The "data" URL scheme. *Internet Requests for Comments* (August 1998), <https://tools.ietf.org/html/rfc2397>
25. Müller, J., Brinkmann, M., Poddebniak, D., Schinzel, S., Schwenk, J.: What’s up johnny? - covert content attacks on email end-to-end encryption. In: *17th International Conference on Applied Cryptography and Network Security (ACNS 2019)*. pp. 1 – 18 (2019)

26. One More Company: State of email with 1.5 billion emails processed. <https://evercontact.com/special/email-tracking.html> (2017)
27. Poddebniak, D., Dresen, C., Müller, J., Ising, F., Schinzel, S., Friedberger, S., Somorovsky, J., Schwenk, J.: Efail: Breaking s/mime and openpgp email encryption using exfiltration channels. In: 27th USENIX Security Symposium (USENIX Security 18). pp. 549–566. USENIX Association, Baltimore, MD (Aug 2018), <https://www.usenix.org/conference/usenixsecurity18/presentation/poddebniak>
28. Roberts, C.: Announcing send time optimization. <https://www.campaignmonitor.com/blog/new-features/2017/05/announcing-send-time-optimization/>, last accessed on 2021-02-20 (2017)
29. Storm, D.: The hidden privacy hazards of html email. <https://strom.com/awards/192.html>, last accessed on 2021-02-01 (2000)
30. The Tor Project: Towards a tor-safe mozilla thunderbird reducing application-level privacy leaks in thunderbird. URL: <https://web.archive.org/web/20200618193439/https://trac.torproject.org/projects/tor/raw-attachment/wiki/doc/TorifyHOWTO/EMail/Thunderbird/Thunderbird%2BTor.pdf>, last checked on 2020-02-02 (July 2011)
31. Voth, C.: Reaper exploit. <http://web.archive.org/web/20011005083819/http://www.geocities.com/ResearchTriangle/Facility/8332/reaper-exploit-release.html>, last accessed on 2020-12-15
32. Xu, H., Hao, S., Sari, A., Wang, H.: Privacy risk assessment on email tracking. In: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. pp. 2519–2527 (April 2018). <https://doi.org/10.1109/INFOCOM.2018.8486432>