The impact of

Machine Generated Emails

On data-driven marketing

lookr

Executive Summary

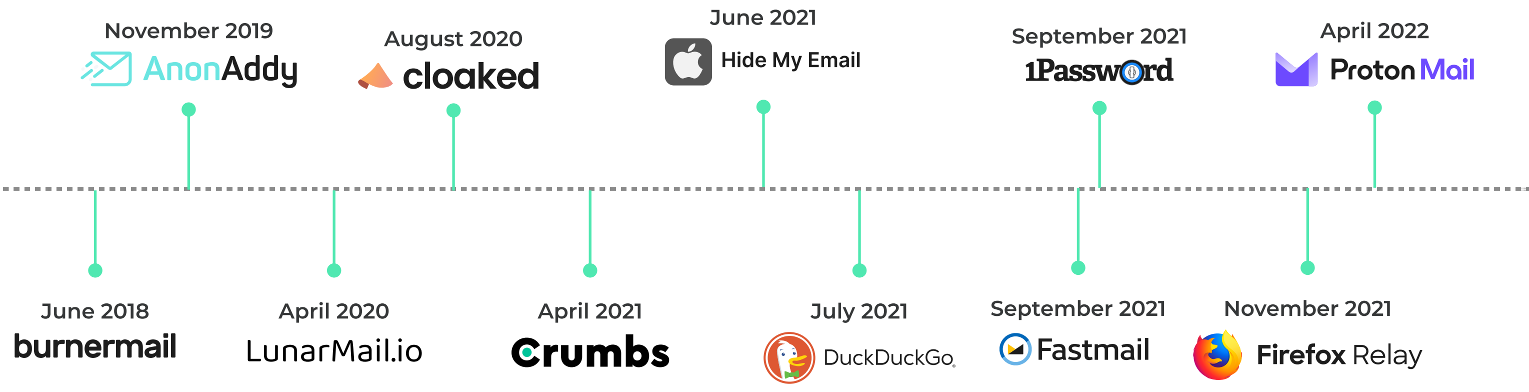
Machine-Generated Emails ("MGEs") are temporary, anonymous email aliases that auto-forward messages to users' real email inboxes.

MGEs are gaining popularity because consumers are fed up with the volume of emails they receive on a daily basis and because of the lack of transparency and control over how their data is being used by companies online. Though seemingly innocuous, MGEs pose a significant threat to the future of the Advertising and Marketing Technology industries by **obfuscating identity and preventing identity matching** across devices and environments. As a result, MGEs are causing a decline in publisher revenues, impacting brand advertising efforts and threatening the future of the open and free web.

What are Machine-Generated Email Services?

A Machine-Generated Email service, such as Apple Hide My Email or Firefox Relay, allows a user to create a *new* email alias for every transaction or digital registration - all of which forward messages to the user's pre-existing email account (Gmail, Outlook, Yahoo, etc.). These aliases can be disabled by the user at any point - meaning when they no longer wish to receive emails from a brand or business, rather than unsubscribe, they disable the email address itself.

One of the most well-known MGE services is Burner Mail which was founded in 2018. The company's nomenclature applies the logic of a "burner phone" (an anonymous and untraceable communication device) to email. Since the founding of Burner Mail, numerous other services have come to market at various price points, with several well-known companies making a play in the space since 2021. Apple launched Hide My Email in June 2021 as part of its iCloud+ subscription. DuckDuckGo, a privacy-first search engine and browser launched its anonymous email forwarding service in beta the following month, and Firefox Relay relaunched with a premium offering (including additional email aliases) in November 2021.



Why are consumers adopting MGEs?

There are several reasons why consumers are adopting Machine-Generated Emails at a greater rate:

Overflowing inboxes

The most significant pressure driving consumers to MGE services is the sheer volume of promotional email received by the average internet user on a daily basis.

Email is the crux of all online transactions - online shopping, newsletter subscriptions, etc. - a necessary give and take that opens a Pandora's box of promotions for years to come. As businesses have come to rely more heavily on email over the past few decades, email has also now become the key for brand loyalty programs.... gone are the days when the local sandwich shop handed out a 10-hole punch card for a free club.

Approximately 306.4 billion

emails were sent and received per day in 2020. Email statistics predict that this number will reach 376.4 billion by 2025.[1]

The issue of inbox overload is only growing, unfortunately. Big Tech companies are in the process of phasing out the “cookie,” causing publishers and brands to shift to email as the new key identifier for online advertising. Industry efforts such as UID 2.0, LiveRamp ATS, and the myriad of data clean room options all rely on an email address to track a user across the web for the purposes of targeted advertising. So, while first party data has always been king, the impending deprecation of the cookie has publishers and marketers desperate for **the one identifier that is not going away: email addresses**. The result is that more and more websites are asking for email and content is often cloaked behind a registration wall. Consumers are forced to divulge their email address at every turn.

Promotional offers

With a focus on email marketing, almost every retail brand offers a one-time discount to new site visitors who provide their email address. Many publishers also offer a free trial or limited access to a certain number of articles each month to draw users in. Consumers who have caught on to these trends inevitably search for ways to game the system. By using a machine-generated email service, consumers can create a unique, anonymous email address for every single purchase or site account, thus they are able to apply a “single-use” discount code, or reactivate a free trial period, again and again. Brands are combatting this with the requirement of a phone number in addition to email - but many MGE services are following suit and adding SMS support that is identical to how the proxy email works.

[1] “Number of e-mail users worldwide 2017-2025”, Statista.com - https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/, November 14, 2022

Ease of Use

Apple's Hide My Email solution in particular is enacting change in consumer behavior by integrating the MGE product directly into iOS natively, as well as in the Safari browser across devices. According to Statista, 48.7% of Smartphone users in the US have an iPhone.[2] As these users, and those utilizing Safari on a desktop device, browse the web and encounter email fields, they are prompted to utilize a Hide My Email alias rather than their own email. The prompt, activated by default, allows the user to generate and input the email alias with just one tap.

Privacy concerns

Finally, there are a growing number of consumers who have concerns around data privacy and who, as a result of unsavory data practices that have been exposed in the past, are hesitant to share their true identity on the web. A recent DataGrail study found that 84% of people want to know which businesses are collecting their data and 77% want control of how that data is being used. That same study noted that 8 out of 10 Americans think there should be a federal law protecting their personal data, and in the absence of legislation, they are taking matters into their own hands. In fact, 87% of consumers have taken action to protect their online privacy, including deleting cookies or browsing history (56%), unsubscribing from email lists (51%), and using ad-blocker apps (32%).[3] As nascent technology, MGEs are not explicitly noted in this study, but using a machine-generated email achieves many of the same results of these actions, including: (1) removing identifiers (2) blocking emails and (3) preventing targeted advertising.

What is the issue with MGEs?

As noted above, the deprecation of the cookie is having resounding effects on the advertising and marketing ecosystems - most notably putting pressure on publishers and brands to build email lists of first party data. But when those email lists include MGEs, the quality, value, and usability of that first party data significantly declines.

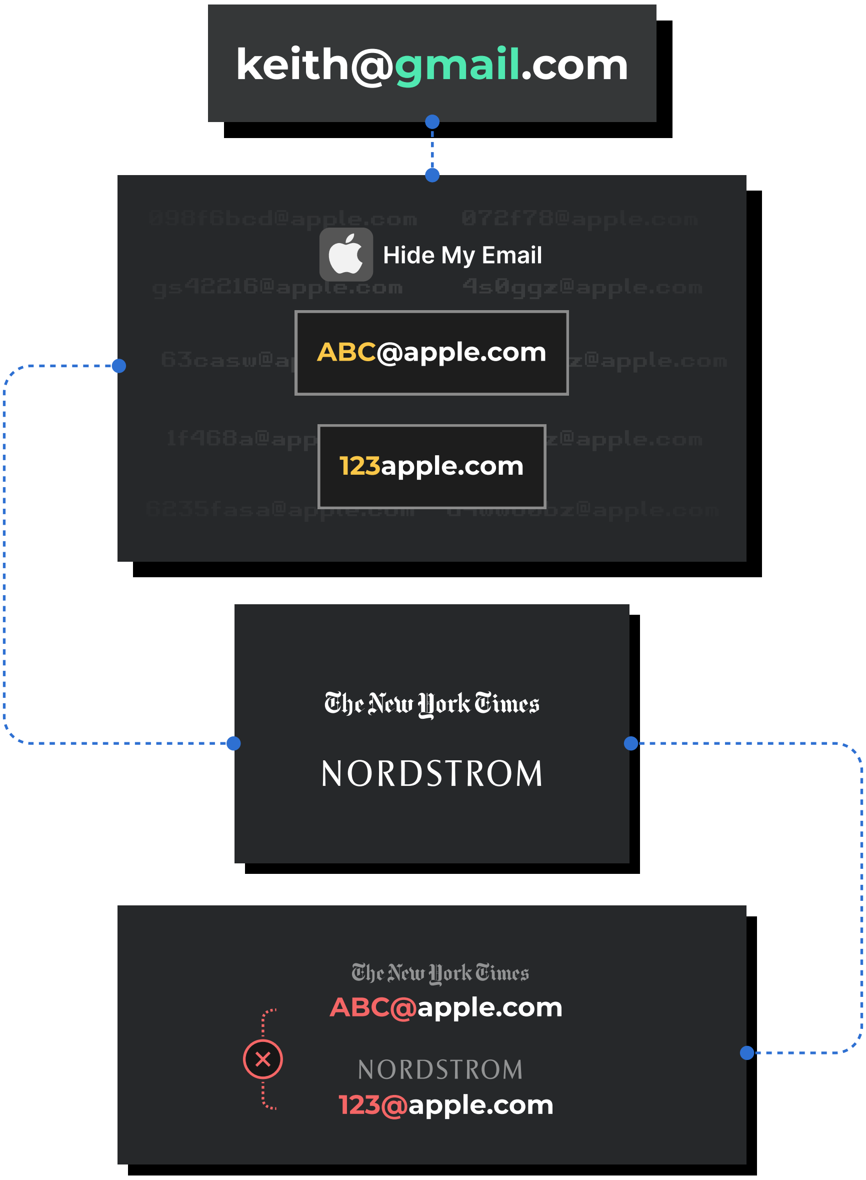
[2] "U.S. iPhone users as share of smartphone users 2014-2022", Statista.com - https://www.statista.com/statistics/236550/percentage-of-us-population-that-own-a-iphone-smartphone/, October 2022

[3] "2022 The Privacy and Ecommerce Report", Datagrail - https://www.datagrail.io/resources/reports/2022-the-privacy-and-ecommerce-report/, 2022

Here's why:

A user with the genuine email address keith@gmail.com decides to use Apple Hide My Email's service to register for an account on the New York Times and to make a purchase on Nordstrom.com. Using Apple Hide My Email, he provides a randomly generated "burner" email address to each site - in this example, ABC@apple.com to NYTimes and 123@apple.com to Nordstrom.

Nordstrom then decides to retarget Keith for an item he perused on the site but did not purchase. Nordstrom loads "Keith's" email address into their advertising platform (123@apple.com) but is unable to locate Keith on any other sites. Keith is currently browsing the NYTimes but he is logged in with a completely unique email (ABC@apple.com) thus Nordstrom (the advertiser) and New York Times (the publisher) have no idea that this is the same user. Moreover, the identity matching platforms also have no clue that Keith is using these aliases. As they encounter these email addresses, they are creating new, unique identifiers for Keith - rather than matching these aliases to his pre-existing identifier that is associated with Keith@gmail.com.



The use of MGEs has completely obfuscated Keith's true identity.

Impact on Publishers

In the above example, the New York Times, a publisher, was unable to capitalize on a targeted advertising opportunity for one of its advertising customers (Nordstrom) due to the inability to match a user ID across the two audience sets. As MGE adoption grows, this problem compounds, creating a significant impact on advertising revenue for publishers.

Studies have shown that the inability for advertisers to reliably target, frequency cap, and attribute impressions on publisher inventory has resulted in a 64% revenue loss for publishers.[4]

But in a cookieless world, publishers that rely on some form of identity in the bid request can expect a CPM lift of up to 142%.[5] These numbers illustrate how critical it is for publishers to have verified, authenticated user emails in their audience.[6] MGEs, as demonstrated above, are completely worthless in the context of identity and advertising.

Beyond lower CPMs, MGEs also create issues with:

Subscriber marketing.

When a site visitor disables an alias, automated emails to re-engage them are not delivered, limiting the ability to drive user traffic back to the site and create more impressions.

Audience development.

Publisher audience lists are becoming muddied with unauthenticated email addresses. As publishers look to monetize those audience segments, buyers are weeding out the unmatched IDs.

Fee-based subscriptions.

MGEs can pose significant risks here as well, especially when a "free trial" period is offered; users simply generate a new email alias when their free trial expires.

[4] "Effect of disabling third-party cookies on publisher revenue", Google - https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf, August 2019

[5] "Mediavine Sees CPM Lift in Cookie-Restricted Browsers Globally with LiveRamp and Index Exchange", Liveramp - https://liveramp.com/mediavine-sees-cpm-lift-cookie-restricted-browsers-globally-with-liveramp-index-exchange/

[6] To illustrate these statistics, here is a simple example:
A given publisher charges a $10 CPM for their inventory. As the industry deprecates cookies, a given impression is worth less to potential advertisers as they cannot tie the impression back to their audience. Thus they are only willing to pay a $3.60 CPM for this anonymous inventory ($10 x (1-64%) = $3.60). By adding a cookieless identifier back to their inventory, match rates increase and publishers increase the value of a given impression by 142%. If we apply this increase to the amended CPM of $3.60, we arrive at an updated CPM of $8.71 ($3.60 x (1+142%) = $8.71). This represents a substantial recovery of revenue loss for publishers and demonstrates the need for publishers to focus on adding quality, matchable identifiers to their inventory.

Impact on Brands

For marketers, the above example is also incredibly relevant. Advertising is often a large expense for brands because it works. With online advertising in particular, brands and marketers have the ability to measure and attribute, backing into a positive ROI for any given advertising campaign. The inability to target or retarget a specific user with an advertising campaign has an impact on top-line revenue in the form of lost sales.

> **Moreover, MGEs are frequently used to abuse promotional offers intended by brands and marketers to be single-use or for new customers only.**

Seamlessly creating a new email alias for every transaction makes it all too easy for consumers to skirt the red tape. Brands are seeing revenue impacts for handing out deep discounts on multiple transactions.

Finally, for brands and retailers with a large focus on email marketing, MGEs pose further problems. A user can disable an email alias at any point meaning that all emails sent to that alias are completely undeliverable. Brands thus have no visibility whatsoever into whether their email is being delivered, viewed or read, which makes it incredibly difficult to evaluate the success of a given email marketing campaign. MGEs have resulted in marginal usability of registration data in re-engagement campaigns or any other downstream efforts.

Impact on Consumers

In the short-term, consumers generally benefit from the use of MGEs. The services allow consumers to obscure their identities online and retain some privacy, to control their inbox, and to make use of "one-time" promotions or "free trials" multiple times over.

Yet they aren't very easy to use and they offer a very limited solution to the consumer problem of inbox management. Many MGE services typically offer a simple UI to turn on and off email aliases.

> **There is no way to redirect to different inboxes, filter messages, or even view messages that have been blocked.**

Once an email alias is disabled, any emails sent to the alias during that time are lost. Furthermore, the complexity of the auto-generated email aliases make them difficult to remember and nearly impossible to use outside of the digital environment.

Impact on the Open and Free Web

There is also another negative consequence of MGEs that will impact all of us, including consumers. While many individuals are quick to complain about intrusive or overly personalized advertising, typically they fail to consider the alternative. The internet was built as an open and free forum - and the free consumption of the content on the web is fueled by advertising. Without advertising revenue, there would be no free local news sites, blogs, or social media. Without advertising, websites would have to switch to subscription-based models, meaning that consumers have to pay for access. Some users may say they are fine with paying a fee and don't mind shelling out a couple bucks a month for the few sites they frequent, but this creates a larger problem:
the fragmentation of information.

If all content on the web sits behind a paywall, consumers will limit their consumption even further to only a handful of websites. As a consequence, many smaller publishers and long-tail sites will be forced out of business. This consolidation and restriction on the free flow of information is dangerous for society in the future.

But what does this have to do with MGEs? Well, MGEs create a complex web of identity for individuals. They prevent marketers and publishers from connecting their audiences for the purposes of targeted advertising, driving down CPMs and tanking ad revenue. As this happens, publishers are forced to cut costs or find new ways to generate revenue, outside of advertising - namely, subscriptions. Paywalls will continue to emerge.

> Machine-Generated Emails pose a significant threat to the future of the open and free web

MGEs are reminiscent of ad blockers. Introduced in 2002, ad blockers were once something only the most ardent ad evaders installed. But that has changed, with as many as 42% of internet users adopting ad blockers.[7] Now, MGEs are threatening advertisers and publishers in the same way that ad blockers have impacted publishers' businesses to date. Simply put, both ad blockers and MGEs interrupt the efficiency of advertising inventory monetization.

How big is the problem?

The issue of machine-generated emails is nascent but growing rapidly. As more MGE solutions come to market and consumer frustration with inbox overload grows, the issue of unauthenticated site traffic will have a ripple effect on first party data strategies.

Through its Identity lockr product, lockr is tracking the frequency of machine-generated emails in aggregate. lockr will be reporting the prevalence and growth of MGEs on a quarterly basis. Updates to the data will be available at www.loc.kr/authenticationtrends and emailed directly to anyone who downloads this white paper.

[7] "Ad Blocker Usage and Demographic Statistics in 2022", Backlinko - https://backlinko.com/ad-blockers-users, March 2021

What about data clean rooms?

The industry is busy preparing for the cookiepocalypse, by assessing a variety of cookieless identity solutions (including Unified ID 2.0 and LiveRamp ATS), CDPs (Customer Data Platforms), and several data clean rooms (where multiple parties can pool their data without ever exposing it in the raw form). But these solutions are not immune to the issues posed by MGEs. If any of these solutions have MGEs in their dataset, there will be a data mismatch. They'll have abc@privaterelay.appleid.com on Nike.com and john@gmail.com on Walmart.com — and all that audience-shaping information will be useless. That data clean room then contains unauthenticated and anonymous email identifiers that undermine the general quality of the data pool and hurt match rates. Plus, these errors cannot be fixed retroactively.

In short, any identity solution that is relying on email addresses is susceptible to the pitfalls of MGEs and the only remedy is to prevent collection of this fallible data in real time.

Conclusion

Email is arguably the most important personal identifier over someone's lifetime. It's the first place many people look in the morning and the last place they go at the end of the day. It's no wonder consumers are reluctant to share their real email addresses. As such, marketers should only expect the adoption of Machine-Generated Email services to grow, and this complex web of identity will leave publishers and retailers without legitimate targeting capabilities and lost revenue.

The advertising industry needs to come together to take a stand against MGEs. To preserve the open and free internet, it is necessary to prevent the usage of MGE services, much as the industry has done for ad blocking services. But it is imperative to address the underlying issues, otherwise this will become a constant game of Whac-A-Mole. Consumers need a way to manage the marketing messages they receive. They need to be able to opt in and out of emails easily. They need to know when they are being retargeted and should be able to opt out of that, too. The entire value exchange of the internet should be redefined so that consumers can control all their own data, all the time. Making sure consumers have complete control, whether it's for traditional media or retail media, is essential.

The future of the Advertising and Marketing Technology industries—and the entire free and ad-supported open Internet—depends on it.

About lockr

lockr was founded in 2020 with the vision to preserve open access to information across the Internet, while honoring consumer privacy and choice. lockr's first consumer product, lockrMail, was released in early 2021 (www.lockrMail.com). lockr launched the B2B side of its business in June 2022 with the release of Identity lockr. lockr is funded by world-class angel investors and venture capital firms.

For more information about lockr and its solutions, please visit www.loc.kr.