Emerging Media Companies, Tracking Cookies, and Data Privacy

an open letter

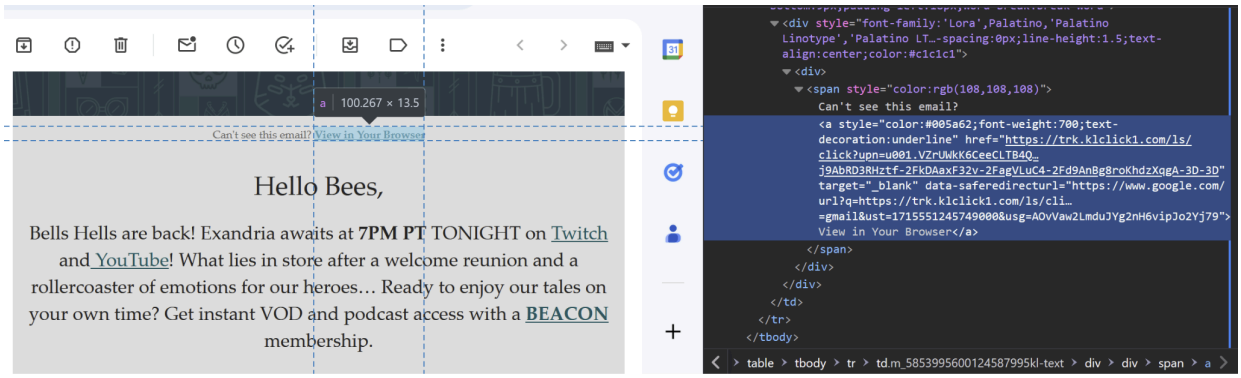
author: era
publish date: 23/05/2024
update date: 23/05/2024

0. TL;DR

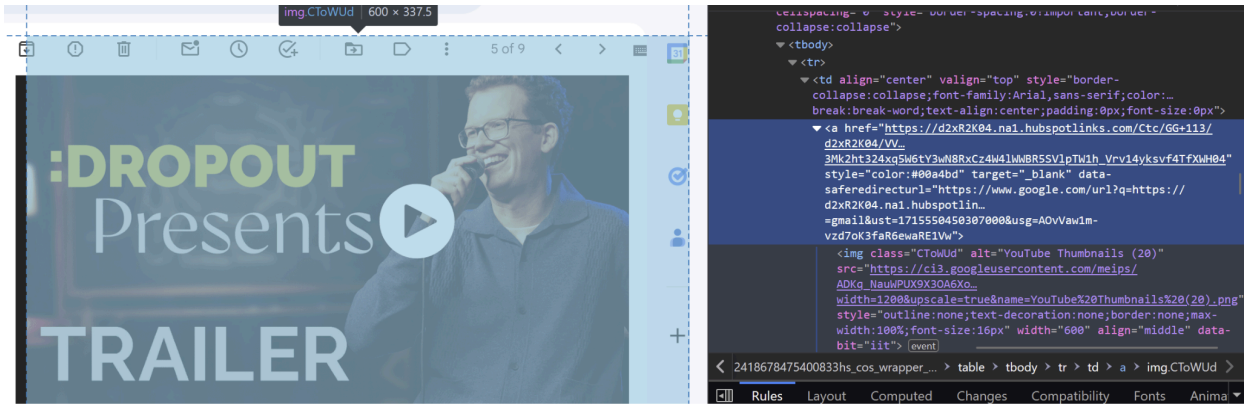
- Both Critical Role (CR) and Dropout are exclusively using links provided by third-party digital marketing solution companies in their email newsletters.
- Every link in each of the newsletters (even the unsubscribe link) goes through a third-party domain which is flagged as a tracking server by the uBlock Origin browser extension.
- Third-party tracking cookies are strictly unnecessary and come with a wide array of risks, including non-consensual targeted advertising, targeted misinformation, doxxing, and the potential for abuse by law enforcement.
- IMO these advertising companies (and perhaps CR/Dropout by proxy) **might be** breaking the law in the EU and California by violating the GDPR and CCPA respectively.
- Even if Critical Role and Dropout are not directly selling or exploiting your personal data, they are still profiting off of it by contracting with, and receiving services from, companies who almost certainly are.
- They should stop.

1. What is happening?

Critical Role and Dropout have begun exclusively using links provided by third-party digital marketing solution companies in their email newsletters.

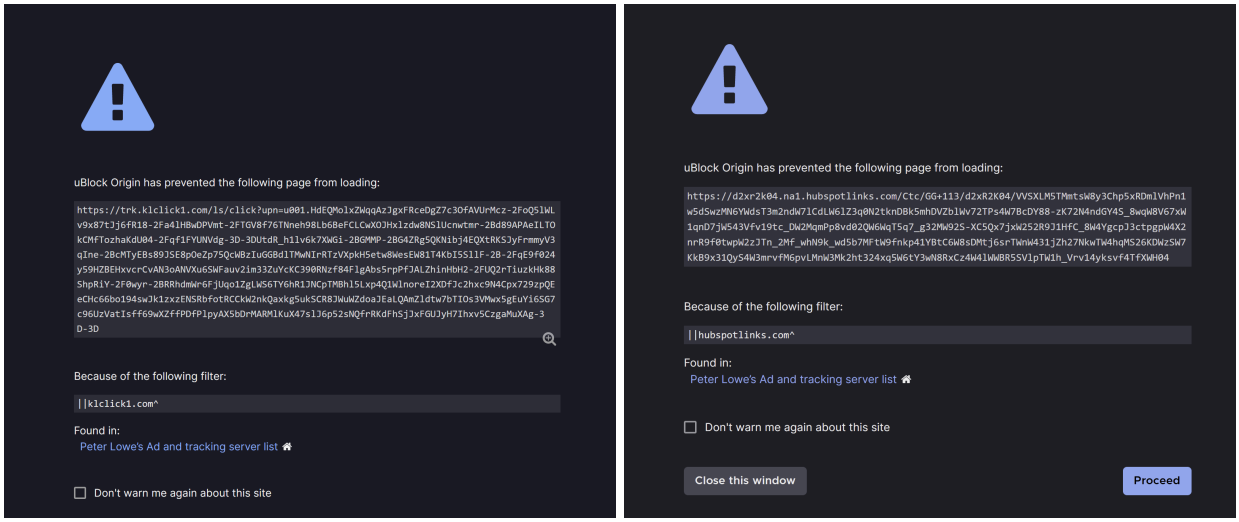


[Description: A screenshot of the CR newsletter alongside the page's HTML source which shows that the target destination for an anchor element in the email leads to trk.klclick.com]



[Description: A screenshot of the Dropout newsletter alongside the page's HTML source which shows that the target destination for an anchor element in the email leads to d2xR2K04.na1.hubspotlinks.com]

The domains attached to these links are flagged as advertising trackers by the uBlock Origin browser extension.



[Description: Screenshots of a Firefox web browser taken after clicking the above links. The page displays a large warning icon and reads “uBlock Origin has prevented the following page from loading [...] because of the following filter: `||klclick1.com` found in Peter Lowe’s Ad and tracking server list.]

In both cases, every link in the newsletter goes through the flagged third-party domain, and the intended endpoint (Twitter, their store page, etc.) is completely obscured and inaccessible from within the email itself. **Even the unsubscribe links feed through the tracking service.**

You can test this yourself in your own email client by hovering your cursor over a link in the email without clicking it and watching to see what URL pops up. You may have noticed this yourself if you use uBlock Origin as an ad-blocker.

I don’t know for certain when this first started. It’s possible that this has been going on for a year or more at this point, or it may have started just a few months ago. Either way: **it ought to stop.**

2. What is a tracking cookie?

> “Never attribute to malice that which can be adequately explained by neglect, ignorance or incompetence.”
> *—Hanlon’s Razor*

A tracking cookie is a unique, universally identifiable value placed on your machine by somebody with the intention of checking for that value later to identify you (or at least to identify your machine).

Tracking cookies are primarily used by companies to create advertising behaviour profiles. These profiles are supposedly anonymous, but even if the marketing companies creating them are not lying about that (a tough sell for me personally, but your mileage may vary when it comes to corporations with 9-figure annual incomes), **the data can often be de-anonymized**. If this happens, the data can be used to identify the associated user, potentially including their full name, email address, phone number, and physical address—all of which may then be associated with things like their shopping habits, hobbies, preferences, the identities of their friends and family, gender, political opinions, job history, credit score, sexuality, and even when they ovulate.

If you are entirely comfortable with the idea of all that data being collected about you and exploited for profit— without your consent—don't click away just yet, because it gets worse.

Now, it is important to note that **not all cookies are tracking cookies**. A cookie is just some data from a webpage that persists on your machine and gets sent back to the server that put it there. Cookies in general are not necessarily malicious or harmful, and are often essential to certain web features functioning correctly (e.g. keeping the user logged in on their web browser after they close the tab). But the thing to keep in mind is that a domain has absolute control over the information that has been stored on your computer by that domain.

This means that criticalrole.com only has access to the information stored on your machine by criticalrole.com and, importantly, *only* criticalrole.com has access to that information. The same is true for trk.klclick1.com and na1.hubspotlinks.com (the URLs currently redirected to by the Critical Role and Dropout newsletter emails, respectively). When your browser goes through one of these domains before redirecting you to the place you *thought* you were going in the first place, **the people who control those domains are the only ones who know for sure what is happening**. You, the user, have no way of knowing or checking and neither does Critical Role/Dropout, aside from trusting that the word of a domain that has been flagged by a widely-used and respected tracker-reporting list (the justifications for a domain's inclusion on which can be found here). You can look at the outgoing information being sent from your machine, but its purpose cannot be determined without knowing what is being done with it on the other side, and these marketing companies ought not to have the benefit of your doubt when they have already been flagged by privacy watchdogs.

You may already have an idea of why all this might be a problem, but if you don't …

3. What's the harm?

Most urgently, as I touched on above: The main source of harm is from corporations profiting off of your private data without your informed consent. However, targeted advertising is actually the *least* potentially harmful outcome of tracking cookies.

I. Data brokers

A data broker is an individual or company that specializes in collecting personal data (such as personal income, ethnicity, political beliefs, geolocation data, etc.) and selling or licensing such information to third parties for a variety of uses, such as background checks conducted by employers and landlords, two universally benevolent groups of people.

There are varying regulations around the world limiting the collection of information on individuals, however **in the jurisdiction of the United States there is no federal regulation protecting consumers from data brokers.** In fact, due to the rising interest in federal regulation, data broker firms lobbied to the tune of $29 million in the year 2020 alone.

(The State of California passed a law attempting to address this problem in 2018, following in the footsteps of the EU's GDPR, but no federal regulation currently exists. See Section 6 for more information.)

II. De-anonymization techniques

Via the use of statistical techniques and powerful computers, 'anonymous' data (that is, data about an individual that is provided without any explicit identification or sensitive information such as their name or address) can often be de-anonymized.

Data re-identification or de-anonymization is the practice of combining datasets (such as advertising profiles) and publicly available information (such as scraped data from social media profiles) in order to discover patterns that may reveal the identities of some or all members of a dataset otherwise intended to be anonymous.

Using the 1990 census, Professor Latanya Sweeney of the Practice of Government and Technology at the Harvard Kennedy School found that up to **87% of the U.S. population can be identified using a combination of their 5-digit zip code, gender, and date of birth.** [Link to the paper.]

Individuals whose data is re-identified are at risk of having their private information concerning finances, health, and preferences sold to organizations without their knowledge or consent. Once an individual's privacy has been breached as a result of re-identification, future breaches become much easier: as soon as a link is made between one piece of data and a person's real identity, that person is no longer anonymous and is at far greater risk of having their data from other sources similarly compromised.

III. Doxxing

Once your data has been de-anonymized, you are significantly more vulnerable to all manner of malicious activity: from scam calls and emails to identity theft to doxxing. This is of particular concern for members of minority groups who may be targeted by hate-motivated attacks.

IV. Potential for abuse by government and law enforcement

Excerpt from "How period tracking apps and data privacy fit into a post-Roe v. Wade climate" by Rina Torchinsky for NPR:

> "Millions of people use apps to help track their menstrual cycles. Flo, which bills itself as the most popular period and cycle tracking app, has amassed 43 million active users. Another app, Clue, claims 12 million monthly active users.
>
> "The personal health data stored in these apps is among the most intimate types of information a person can share. And it can also be telling. The apps can show when their period stops and starts and when a pregnancy stops and starts.
>
> "That has privacy experts on edge because this data—whether subpoenaed or sold to a third party—could be used to suggest that someone has had or is considering an abortion.
>
> "'We're very concerned in a lot of advocacy spaces about what happens when private corporations or the government can gain access to deeply sensitive data about people's lives and activities,' says Lydia X. Z. Brown, a policy counsel with the Privacy and Data Project at the Center for Democracy and Technology. 'Especially when that data could put people in vulnerable and marginalized communities at risk for actual harm.'"

So why have I included this? Obviously Critical Role and Dropout are not collecting any sort of data related to their users' menstrual cycles. But the thing to keep in mind is that **any data** of

yours that is exposed to third parties **can be sold and distributed without your knowledge or consent** and then be used by disinterested—or outright malicious—actors to de-anonymize your data from other sources, included potentially highly compromising data such as that collected by parties such as these period-tracking apps. Data privacy violations have compounding dangers, and should be proactively addressed wherever possible.

V. Targeted misinformation

Data brokers are often incredibly unscrupulous actors, and will sell your data to whomever can afford to buy it, no questions asked. The most high-profile case of the consequences of this is the Facebook—Cambridge Analytica data scandal, wherein the personal data of Facebook users were acquired by Cambridge Analytica Ltd. and compiled alongside information collected from other data brokers. By giving this third-party app permission to acquire their data back in 2015, Meta (then Facebook) also gave the app access to information on their users' friend networks: this resulted in the data of some 87 million users being collected and exploited.

The data collected by Cambridge Analytica was widely used by political strategists to influence elections and, by and large, undermine democracy around the world: While its parent company SCL had been influencing elections in developing countries for decades, Cambridge Analytica focused more on the United Kingdom and the United States. CEO Alexander Nix said the organization was involved in 44 American political races in 2014. In 2016, they worked for Donald Trump's presidential campaign as well as for *Leave.EU,* one of the organisations campaigning for the United Kingdom to leave the European Union.

VI. The Crux: Right to Privacy Violations

Even if all of the above were not concerns, **every internet user should object to being arbitrarily tracked on the basis of their right to privacy**. Companies should not be entitled to create and profit from personality profiles about you just because you purchased unrelated products or services from them. This right to user privacy is the central motivation behind laws like the EU's GDPR and California's CCPA (see Section 6).

4. Refuting Common Responses

I. “Why are you so upset? This isn’t a big deal.”

Commenter: *Oh, if you’re just talking about third party cookies, that’s not a big deal … Adding a cookie to store that ‘this user clicked on a marketing email from critical role’ is hardly [worth worrying about].*

Era*: I don’t think you understand what tracking cookies are. They are the digital equivalent of you going to a drive through and someone from the restaurant running out of the store and sticking a GPS monitor onto your car.*

Commenter: *Kind of. It’s more like slapping a bumper sticker on that says, in restaurant-ese, ‘Hi I’m [name] and I went to [restaurant] once!’*

This is actually an accurate correction. My metaphor was admittedly overly simplistic, but the correction specifies only so far as is comfortable for the commenter. If we want to construct a metaphor that is as accurate as possible, it would go something like this:

You drive into the McDonald’s parking lot. As you are pulling in, unbeknownst to you, a Strange Man pops out of a nearby bush (that McDonald’s has allowed him to place here deliberately for this express purpose), and sticks an invisible bumper sticker onto the back of your car. The bumper sticker is a tracker that tells the Strange Man which road you took to drive to McDonald’s, what kind of car you drive, and what (if anything) you ordered from McDonald’s while you were inside. It might also tell him where you parked in the parking lot, what music you were listening to in your car on the way in, which items you looked at on the menu and for how long, if you went to the washroom, which washroom you went into, how long you were in the washroom, and the exact location of every step you took inside the building.

Now, as soon as you leave the McDonald’s, the bumper sticker goes silent and stops being able to report information. But, let’s say next week you decide to go to the Grocery Store, and (again, unbeknownst to you), the Strange Man *also* has a deal with the Grocery Store. So as you’re driving into the grocery store’s parking lot, he pops out of another bush and goes to put another bumper sticker onto your car. But as he’s doing so, he notices the bumper sticker he’s already placed there a week ago that only he can see (unless you’ve done the car-equivalent of clearing your browser cache), and goes “ah, it’s Consumer #1287499290! I’ll make sure to file all of this new data under my records for Consumer #1287499290!”

You get out of your car and start to walk into the Grocery Store, but before you open the door, the Strange Man whispers to the Grocery Store: “Hey, I know you’re really trying to push your cereal right now, want me to make it more likely that this person buys some cereal from you?” and of course the Grocery Store agrees—this was the whole reason they let him set up that weird parking lot bush in the first place.

So the Strange Man runs around the store rearranging shelves. He doesn’t know your name (all the data he collects is strictly anonymous after all!) but he does know that you chose the cutesy toy for your happy meal at McDonald’s, so he changes all of the cereal packaging labels in the store to be pastel-coloured and covered in fluffy bears and unicorns. And *maybe* you were already going to the Grocery Store to buy cereal, and *maybe* you’re actually very happy to buy some cereal in a package that seems to cater specifically to your interests, but wouldn’t you feel at least a little violated if you found out that this whole process occurred without your knowledge? Especially if you felt like you could trust the people who owned the Grocery Store? They’re not really your friend or anything, but maybe you thought that they were compassionate and responsible members of the community, and part of the reason that you shopped at their store was to support that kind of business.

II. “Everyone does it, get over it.”

Commenter: *[The marketing company working with CR] is an industry standard at this point, particularly for small businesses. Major partner of Shopify, a fairly big player. If you don't have a software development team, using industry standard solutions like these is the easy, safe option.*

This sounds reasonable, but it actually makes it *worse*, not better, that Critical Role and Dropout are doing this. All this excuse tells me is that most businesses using Shopify (or at least the majority of those that use its recommended newsletter service) have a bush for the Strange Man set up in their parking lot.

Contracting with these businesses is certainly the easy option, but it is decidedly *not* the safe one.

III. “They need to do it for marketing reasons.”

Commenter 1: *Email marketing tools like [this] use tracking to measure open and click rates. I get why you don’t want to be tracked, but it’s very hard to run a sizeable email newsletter without any user data.*

Commenter 2: *I work in digital marketing … every single email you get from a company has something similar to this. Guaranteed. This looks totally standard.*

I am a web programmer by trade. It is my full time job. Tracking the metrics that Critical Role and Dropout are most likely interested in *does not* require embedding third-party tracking cookies in their fans' web browsers. If you feel comfortable taking my word on that, you can skip the next section. If you're skeptical (or if you just want to learn a little bit about how the internet works) please read on.

5. Tracking cookies are never necessary

> "We live in a technocracy. We live in a world in which technology design dictates the rules we live by. We don't know these people, we didn't vote for them in office, there was no debate about their design. But yet, the rules that they determine by the design decisions they make—many of them somewhat arbitrary—end up dictating how we will live our lives."
> *—Latanya Sweeney*

I. What is a website?

A website is a combination of 2 computer programs. One of the two programs runs on your computer (laptop/desktop/phone/etc.) and the other runs on another computer somewhere in the world. The program running on your computer is the **client** program. The program running on the other computer is the **server** program.

II. Requests & Responses

A message sent from the client to the server is a **request**. A message sent from the server to the client is a **response**.

III. Cookies

Cookies are bits of data that the server sends to the client in a response that the client then sends back to the server as an attachment to its subsequent requests.

IV. Sessions

A session is a series of sequential interactions between a client and server. When either of the two programs stops running (e.g. when you close a browser tab), the session is ended and any future interactions will take place in a new session.

V. URLs

A URL is a **U**niform **R**esource **L**ocator. You may also sometimes see the initialism URI—in which the 'I' stands for **I**dentifier—but they effectively refer to the same thing, which is the place to find a specific thing on the internet. For our purposes, a "link" and a URL mean the same thing.

VI. What do Critical Role and Dropout want?

These media companies (in my best estimation) are contracting with the digital advertising companies in order to get one or more of the following things:

1. Customer identity verification (between sessions)
2. Marketing campaign analytics
3. Customer preference profiles
4. Customer behaviour profiles

VII. How can they get these things without tracking cookies?

1. Accounts.
    a. Dropout has an account system already. As Beacon is a thing now I have to assume Critical Role does as well, therefore this is literally already something they can do without any additional parties getting involved.
2. URL Query Parameters.
    a. So you want to know which of your social media feeds is driving the most traffic to your storefront. You *could* contract a third-party advertising company to do this for you, but as we have seen this might not be the ideal option. Instead, when posting your links to said feeds, attach a little bit of extra text to the end of the URL link so: <https://yoursite.blah/store> becomes <https://yoursite.blah/store?campaign=twitter> or <https://yoursite.blah/store?campaign=newsletter> or even <https://yoursite.blah/store?campaign=newsletter&variant=2>
    b. These extra bits of information at the end of a URL are **query parameters**, and act as a way for the client to specify some instructions for the server when sending a request. In effect, a URL with query parameters allows the client to say

to the server “I want *this thing* under *these conditions*”. The benefit of this approach is, of course, that you actually know precisely what information is being collected (the stuff in the parameters) and precisely what is being done with it, and you’ve avoided exposing any of your user data to third parties.

3. Internal data collection.
    a. Optionally associate a user’s email address with their preferences on the site. Prompt them to do this whenever they purchase anything or do any action that might benefit from having some saved preference, informing them explicitly when you do so and giving them the opportunity to opt-out.
4. Internal data collection.
    a. You *can* directly track user behaviour on your website down to every single mouse movement if you really want to—again, no need to get an outside party involved to snoop on your fans. But you shouldn’t do that because it’s a little creepy!

It will of course be more work to set up and maintain these things, and thus it will inevitably be more expensive—but that discrepancy in expense represents **profit that they are currently making on the basis of violating their fans’ right to privacy**.

6. Breaking the Law (GDPR and CCPA)

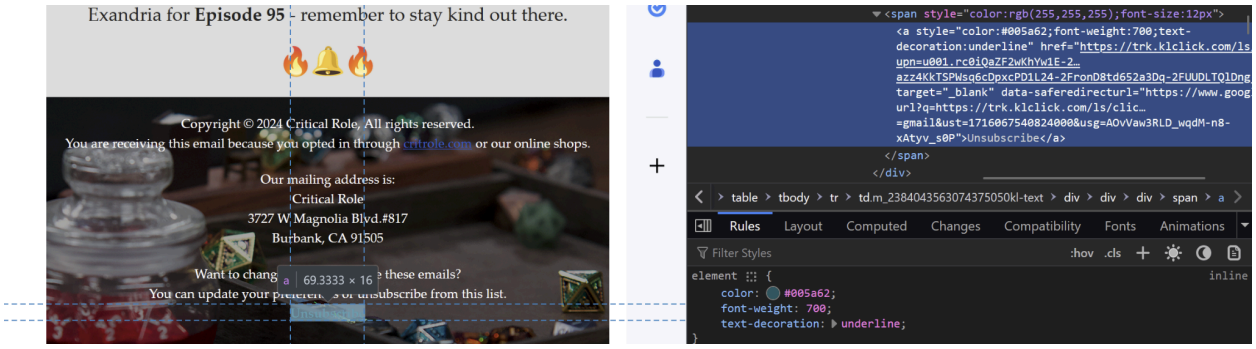
> “Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.”
> — GDPR Art. 21 Section 2

Nobody wants to break the law and be caught. I am not accusing anyone of anything and this is just my personal speculation on publicly-available information. I am not a lawyer; I merely make computer go beep-boop. If you have any factual corrections for this or any other section in this document please leave a comment and I will update the text with a revision note. Before I try my hand at the legal-adjacent stuff, allow me to wade in with the tech stuff.

Cookies are sometimes good and sometimes bad. Cookies from someone you trust are usually good. Cookies from someone you don’t know are occasionally bad. But you can take proactive measures against bad cookies. You should **always** default to denying any cookies that go beyond the “essential” or “functional” categorizations on any website of which you are remotely suspicious. Deny as many cookies as possible. Pay attention to what the cookie pop-ups actually

say and don't just click on the highlighted button: it is usually "Accept All", which means that tracking and advertising cookies are fair game from the moment you click that button onwards. It is illegal for companies to arbitrarily provide you a worse service for opting out of being tracked (at least it is in the EU and California).

It is my opinion (and again, I am not a legal professional, just a web developer, so take this with a grain of salt) **that the links included in the newsletter emails violate both of these laws**. If a user of the email newsletter residing in California or the EU wishes to visit any of the links included in said email without being tracked, *they have no way of doing so*. None of the actual endpoints are available in the email, effectively forcing the user to go through the third-party domain and submit themselves to being tracked in order to utilize the service they have signed up for. Furthermore, it is *impossible to unsubscribe* directly from within the email without also submitting to the third-party tracking:



[Description: A screenshot of the 'unsubscribe' button in the CR newsletter alongside the page HTML which shows that the target destination for the anchor element is a trk.klclick.com page.]

As a brief aside: Opening the links in a private/incognito window is a good idea, but will not completely prevent your actions from being tracked by the advertiser. My recommendation: install uBlock Origin to warn you of tracking domains (it is a completely free and open-source project available on most major web browsers), and do not click on any links in either of these newsletters until they change their practices.

Now, it may be the case that the newsletters are shipped differently to those residing in California or the EU (if you are from either of these regions please feel free to leave a comment on whether or not this is the case), but ask yourself: does that make this any better? Sure, maybe then Critical Role and Dropout (or rather, the advertising companies they contract with) aren't *technically* breaking the law, but it shows that the only thing stopping them from exploiting your personal data is potential legal repercussions, rather than any sort of commitment to your right to privacy. But I expect that the emails are not, in fact, shipping any

differently in jurisdictions with more advanced privacy legislation—it wouldn't be the first time a major tech giant blatantly flaunted EU regulations.

Without an additional browser extension such as uBlock Origin, a user clicking on the links in these emails may not even be aware that they have interacted with the advertising agency at all, let alone what sort of information that agency now has pertaining to them, nor do they have any ability to opt out of this data collection.

For more information about your right to privacy—something that only those living in the EU or California currently have—you can read explanations of the legislations at the following links (take note that these links, and all of the links embedded in this paper, are anchored directly to the destinations they purport to be, and do not sneakily pass through an additional domain before redirecting you):
https://gdpr-info.eu/
https://oag.ca.gov/privacy/ccpa

7. Conclusion

The important thing to make clear here is this: Even if Critical Role and Dropout are not directly selling or exploiting your personal data, they are still profiting off of it by contracting with, and receiving services from, companies whom I believe are. You may not believe me.

I do not believe that the management teams at Critical Role and Dropout are evil or malicious. Ignorance seems to be the most likely cause of this situation. Someone at some marketing company told them that this type of thing was helpful, necessary, and an industry standard, and they had no reason to doubt that person's word. Maybe that person had no reason to doubt the word of the person who told them. Maybe there are a few people in that chain, maybe quite a few. I do not expect everyone running a company to be an expert in this stuff (hell, I'm nowhere close to being an expert in this stuff myself—I only happened to notice this at all because of a browser extension I just happened to have installed to block ads), but what I do expect is that they change their behaviour when the potential harms of their actions have been pointed out to them, which is why I have taken the time to write this.

PS. To the employees of Critical Role and Dropout

It is my understanding that these corporations were both founded with the intention of being socially responsible alongside turning a profit. By using services like the ones described above, you are, however unintentionally, profiting off of the personal datasets of your fans that are

being compiled and exploited without their informed consent. You cannot say, implicitly or explicitly, “We’re not like those other evil companies! We care about more than just extracting as much money from our customers as possible!” while at the same time utilizing these services, and it is my hope that after reading this you will make the responsible choice and stop doing so.

Thank you for reading,
era