

[see [this article](#) for full explanation]

# Is MailChimp Spyware?

## The issue

MailChimp is increasingly popular in Ireland, and globally – “It has 7 million users that collectively send over 10 billion emails through the service each month,” according to Wikipedia.

I sign up fairly frequently to various services online. Some of these services send regular mailshots, and some of those mailshots use MailChimp. Some of these services are in Ireland. A while back I had reason to look at the source code of one mailshot e-mail. A small part of it looked something like this:

```
<img src=3D"http://iculture.us10.list-manage.com/track/open.php?u=3D94=c96de60e405a9d23796d944&id=3D828f67bcd8&e=3D6ebba7675d" height=3D"1" width=h=3D"1">
```

(The ‘=’ signs and things like ‘3D’ have been inserted by the mail program at the receiving end and are not part of the original mailshot code. The above code is from a MailChimp mailshot I sent myself on 12 March 2015 – see below.)

It’s pretty clear that identifying codes – such as “3D828f67bcd8” – are being used in the e-mail bodies. In this case, an image tag is sending back the “3D828f67bcd8” to a server. The server can then record that I have seen that image, which in turn indicates that I have opened the e-mail. The program on the server is called ‘open.php’ in the directory ‘track’.

## Test account

To confirm that MailChimp is indeed taking information from me without asking, I set up a test account (12 March 2015). I created a 'campaign' (called 'Test') and sent the mailshot to two of my own e-mail addresses. I then checked the reports offered by MailChimp. Had I opened the e-mails? The screenshot below from mailchimp.com shows that I had:

Overview **Activity** ▾ Links Social eCommerce360 Conversations Analytics360

### Opened

Export as CSV

Email Address	Opens	First Name	Last Name	Member Rating	Last Changed
info@paintfor.me >	4	Paint	ForMe	★★★★★	3/12/15 12:35AM
info@dnote.info >	3	Dnote	DotInfo	★★★★☆	3/12/15 12:35AM

And it shows when I looked at the e-mail too:

Overview **Activity** ▾ Links Social eCommerce360 Conversations Analytics360

### Subscriber activity for: [info@dnote.info](#)

03/12/2015

12:42AM

Open

12:50AM

Open

4:15PM

Open

Had I followed the link in the body of the e-mail? MailChimp knew I had, in one of the e-mails:

## Links Clicked

Export as CSV



Any instance of: <http://www.dnote.website>

Email Address	Clicks	First Name	Last Name	Member Rating	Last Changed
info@paintfor.me >	1	Paint	ForMe	★★★★☆	3/12/15 12:35AM

I wasn't surprised – it confirmed what I already suspected, and in any event it is stated clearly on the MailChimp website:

## Tracking



### Track opens

Discover who opens your campaigns by tracking the number of times an invisible web beacon embedded in the campaign is downloaded. [Learn more](#)



### Track clicks Required on free accounts

Discover which campaign links were clicked, how many times they were clicked, and who did the clicking.



### Track plain-text clicks Required on free accounts

Track opens and clicks in the plain-text version of your email by replacing all links with tracking URLs. [Learn more](#)

So not only is this tracking up-front, for MailChimp clients, it's mandatory on free (i.e., small) accounts.\* There's also some enhancement which I didn't try out:



### ClickTale link tracking

Gain insight to how subscribers interact with your email content. Requires [ClickTale](#) on your website.

And there's location tracking:

- **Top locations**

Displays where in the world your subscribers are opening your campaigns. We use [geolocation tracking](#) to collect your subscribers' location information and the name of the country subscribers are from.

This may just be at a country level. However, any request to the MailChimp server – as in when the user opens the mail and the hidden image reports back to MailChimp – is tagged with the user's IP address; this is normal internet protocol. If Google and MailChimp are sharing data, a user could be tracked to a specific physical location using the IP address.

## How is it done?

I've already indicated above that user tracking is done through the images used in the mailshot. Here is MailChimp itself saying how it works (at <http://blog.mailchimp.com/how-gmails-image-caching-affects-open-tracking/>):

You may know this already, but along with most ESPs, MailChimp tracks opens by placing a tiny, single-pixel-sized image in each email. When someone views images in the email, our image-hosting servers get a request for the pixel-sized pic, and we use that request to track opens for each subscriber.

This “placing a tiny, single-pixel-sized image in each email” certainly sounds like an intention to deceive, or at least to be very sneaky.

## Relevance?

What MailChimp gets up to is its own business, literally. Is that also the case, though, if an Irish firm uses MailChimp to send me a mailshot? The firm will know whether I opened the mailshot, how often I did so, and whether I clicked on any of the links. In theory at least I will have signed up to receive the mailshot, but I am not aware of ever agreeing, anywhere that I signed up for a newsletter or registered on a site, to be snooped on in terms of opening e-mails and clicking links. What is more, I may have signed up before the firm was using MailChimp.

‘Integration packages’ offered by MailChimp include SurveyMonkey, Eventbrite, Salesforce, PayPal, and many others. For PayPal, for example, you can “update your list with each new purchase.” With these integration packages there is likely to be a significant disconnect between what the user does – buys something, for example – and later mailshots that can track the user’s behaviour.

Paid-up users of MailChimp can remove MailChimp branding from their mailshots, so the recipient would have no easy way of knowing s/he was dealing with a MailChimp mailshot.

## Two Irish examples

Fáilte Ireland

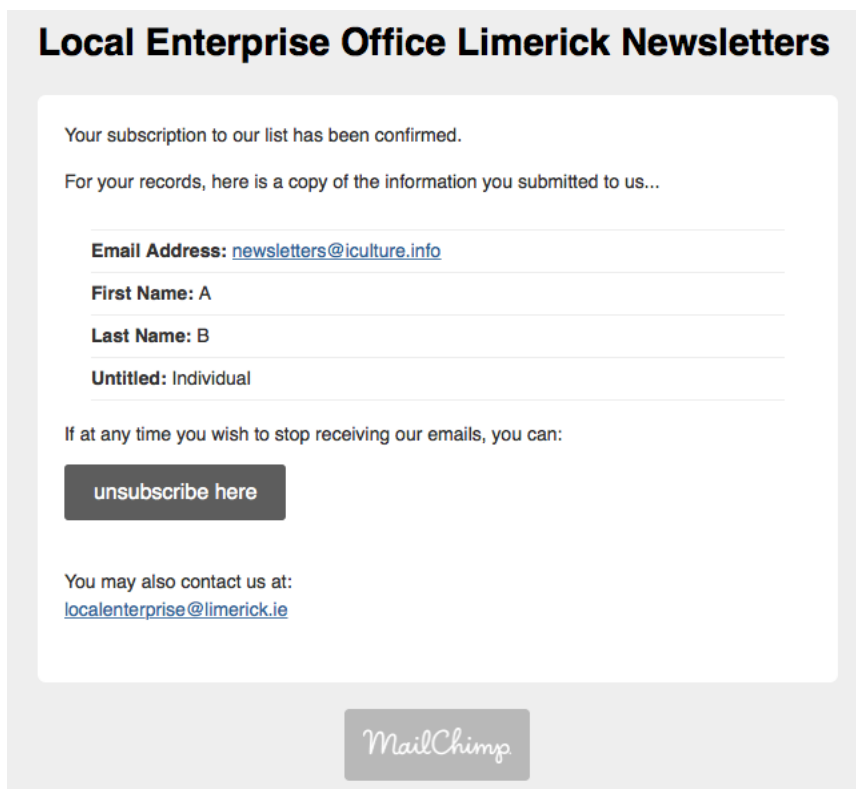
MailChimp is promoted by Fáilte Ireland ([here](#)). And Fáilte Ireland has its own newsletter sign-up, [here](#). To the left on the newsletter sign-up page there is [Privacy and Cookies Policy](#). It would be huge stretch, though, to believe that this policy is informing the user that their e-mail behaviour will be snooped on.

## Local Enterprise Offices

I don't wish to single out LEOs – the use of MailChimp is widespread, it just happens that LEOs turned up in a Google search.

Some LEOs send out newsletters, for which a user can sign up. The site does have 'Legal' right at the bottom of each page (one example is [here](#)), but the information on the Legal page relates only to the website and to direct communications by e-mail *to* the LEO offices; there is no information on privacy in newsletters.

This is what I received after signing up for one LEO newsletter:



It's via MailChimp, so the Limerick LEO can track my behaviour in relation to this e-mail. I haven't received the newsletter itself yet.

## Questions

The above analysis seems to come down to three questions:

1. Is it allowable in Ireland for me to send another person in Ireland an e-mail and receive automatic notification as to whether, when and how often they looked at it, and whether they clicked on any links in it, without their knowing and without their permission?
2. Does it matter whether the e-mail is a one off from myself, or part of a mailshot?
3. Do the answers to the above (1 and 2) change if I route through a server outside of Ireland, although I'm in Ireland?

---

\* Note (this was not in the PDF sent to the Data Protection Commissioner's Office): I was wrong in this assertion – 'Track Opens' is the default, rather than compulsory.