PUBLISHED VERSION

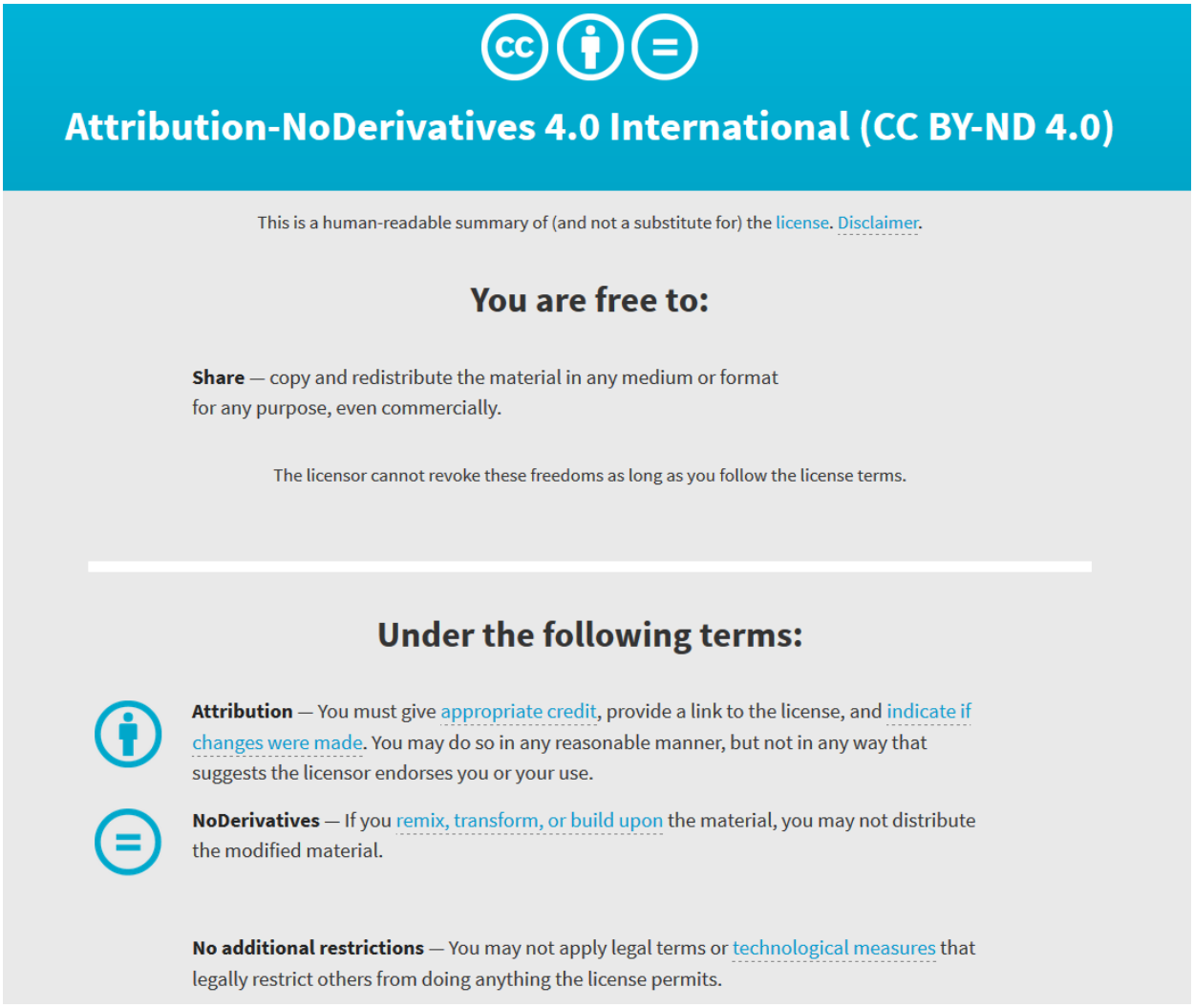
Richard Matthews
How silent signals from your phone could be recording and tracking you
The Conversation : academic rigour, journalistic flair, 2018; Available online May 10, 2018

Copyright © 2017 the Author(s). This publication is available under a Creative Commons Attribution NoDerrivatives licence (CC BY-ND 4.0).

Published version https://theconversation.com/how-silent-signals-from-your-phone-could-be-recording-and-tracking-you-94978

PERMISSIONS

https://creativecommons.org/licenses/by-nd/4.0/



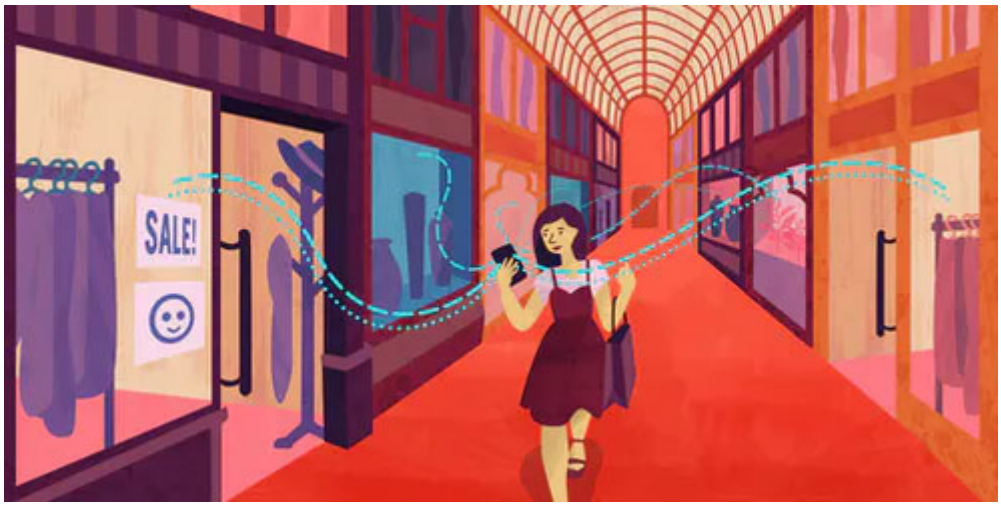
20 October 2020

http://hdl.handle.net/2440/128561

Close

THE CONVERSATION

Academic rigour, journalistic flair



Advertisers may track a customer's shopping preferences within a shopping centre by using ultrasonic beacons emitted from their mobile phones. Mai Lam/The Conversation NY-BD-CC, CC BY-SA

How silent signals from your phone could be recording and tracking you

May 10, 2018 12.01pm AEST •Updated May 11, 2018 9.42am AEST

My lounge room is bugged. My phone is broadcasting an ultrasonic signal to my blu-ray player via an acoustic side channel beyond human hearing.

The channel networks the two devices, similar to how a dial-up connection used to get our computers online before the days of the NBN. The same technology is behind Google's Nearby API through their Eddystone protocol, and is the basis of products sold by the startup Lisnr. It's also the reason more and more apps are requesting access permissions to your microphone.

Author

Richard Matthews
PhD Candidate, University of Adelaide

Read more: Can sound be used as a weapon? 4 questions answered

Aside from networking, companies use ultrasonic signals (or beacons) to gather information about users. That could include monitoring television viewing and web browsing habits, tracking users across multiple devices, or determining a shopper's precise location within a store.

Get news that's free, independent and based on evidence.

Get newsletter

They use this information to send alerts that are relevant to your surroundings – such as a welcome message when you enter a museum or letting you know about a sale when you pass by a particular store.

But since this technology records sound – even if temporarily – it could constitute a breach of privacy. An analysis of various Australian regulations covering listening devices and surveillance reveals a legal grey area in relation to ultrasonic beacons.

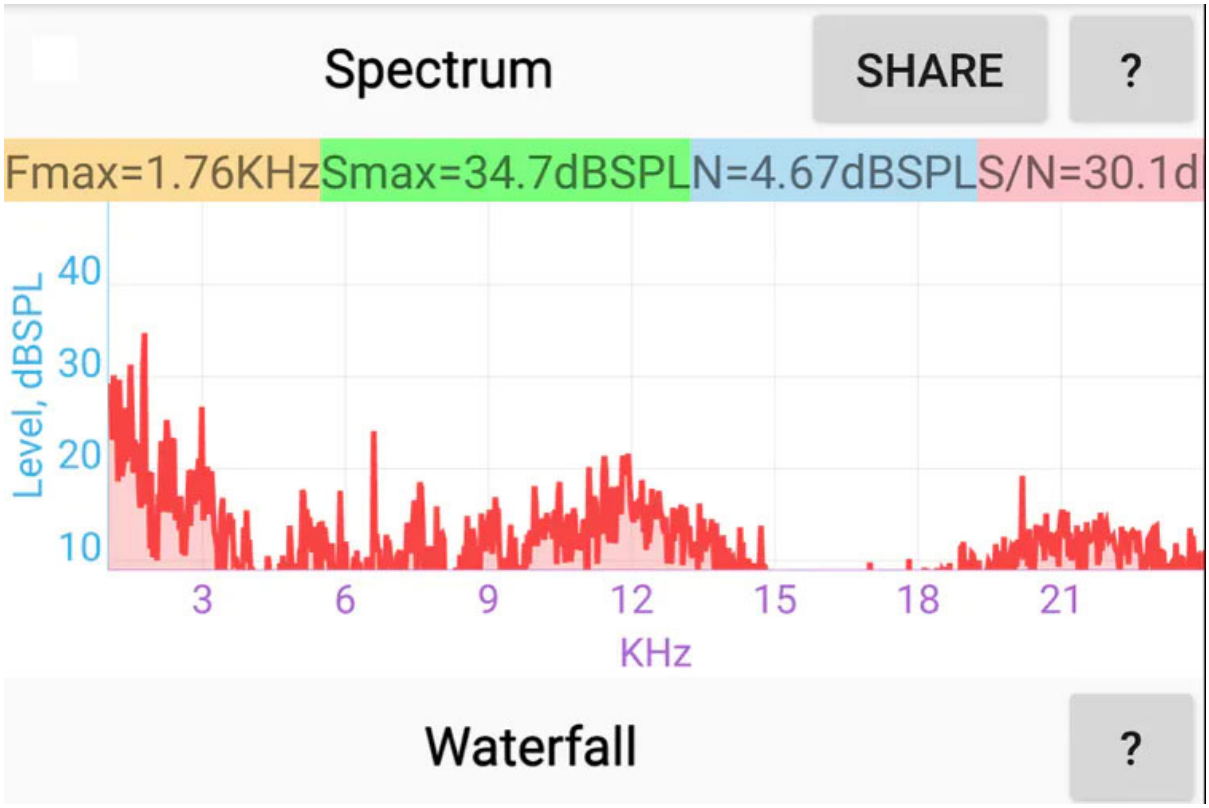
How does ultrasonic data transfer work?

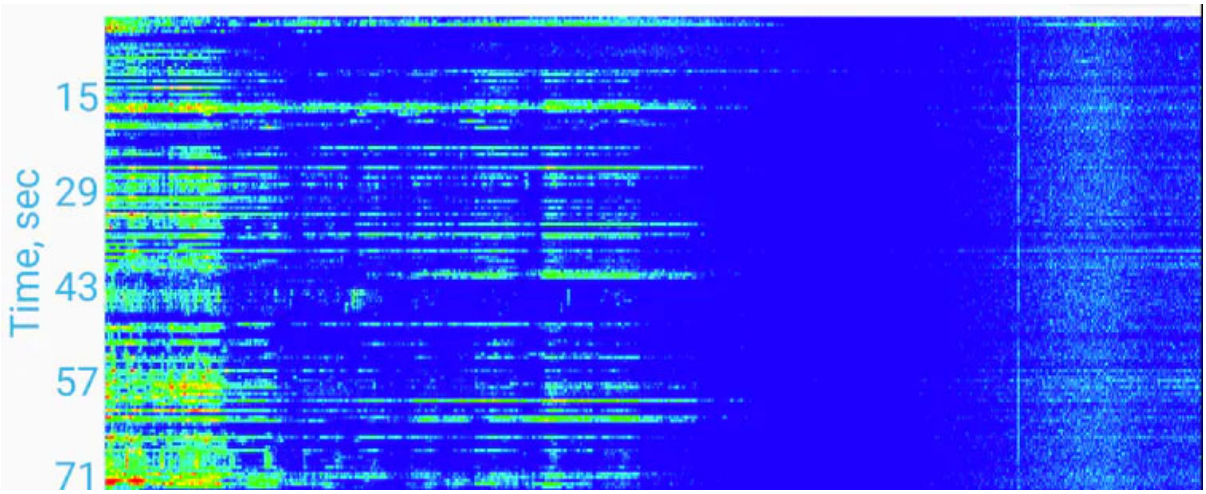
Google Nearby enables Android phone users who are in close proximity to each other to connect their devices and share data, such as documents or media. Google says:

> *To share and collaborate in apps, Nearby uses Bluetooth, Wi-Fi, and inaudible sound to detect devices around your device. (Some people can hear a short buzz.)*

These inaudible sounds are ultrasonic beacons transmitting data that is then picked up by your phone.

To demonstrate this technology, I recorded such a beacon being broadcast in my lounge room while watching Netflix. In the below image you can see the audio ends around the 15kHz mark with the ultrasonic beacon beginning at 20kHz, the point at which average human hearing ends.





Audio capture demonstrating the different frequencies over a 71 second period while watching Netflix. The ultrasonic beacon is apparent in the right hand side of the waterfall diagram.

Since these ultrasonic sounds are the only relevant section of the data signal, it is necessary to remove the lower frequency audible signals (such as speech) that are also captured. This is done by using a high-pass filter. A high-pass filter extracts high frequencies to remain in the data and eliminates the lower frequencies.

This means, in theory, that while the device could be recording sound, it isn't keeping the parts of the recording that might include conversation.

Different filters process signals in different ways. While filters constructed from basic electrical components do not require any storage of the signal, digital software filters require the signal to be stored temporarily.

Is this kind of recording legal?

In South Australia, where I am based, a listening device is precisely defined as:

> *a device capable of being used to listen to or record a private conversation or words spoken to or by any person in private conversation (...) but does not include a device being used to assist a person with impaired hearing to hear sounds ordinarily audible to the human ear.*

There is no exemption provided for recording sounds and then removing the audible portion.

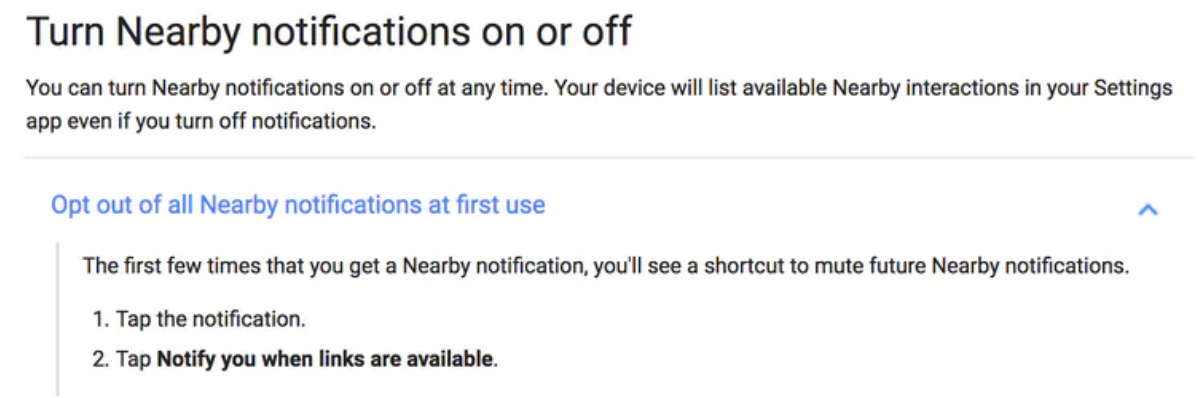
It is generally unlawful "to overhear, record, monitor or listen to a private conversation" unless you have the express permission of all parties involved. Since audio is being recorded using a standard microphone in the course of an ultrasonic data transfer, the full audio spectrum – including any conversation occurring – is being sampled at the same time.

Read more: Your mobile phone can give away your location, even if you tell it not to

---

The type of filter used is therefore critical. If a digital filter is being used to extract the ultrasonic data, the temporary storage of the full audio spectrum could be considered a recording. And that requires consent.

Google gives users the chance to opt-out the first time notifications are made using the Nearby service. However, this could only be construed as consent for the phone owner, not all parties to a possible conversation being recorded in private. Also, by the time the notification happens, the recording has already occurred.



Google's FAQ explaining the opt-out process for the Nearby API.

What about location tracking?

Advertisers can use ultrasonic signals that speak to your mobile phone to establish where you are within a store. They can also correlate this data with other advertising metadata easily obtained from cookies to track your broader movements.

This further complicates matters regarding their legality.

In South Australia, a tracking device is explicitly defined as:

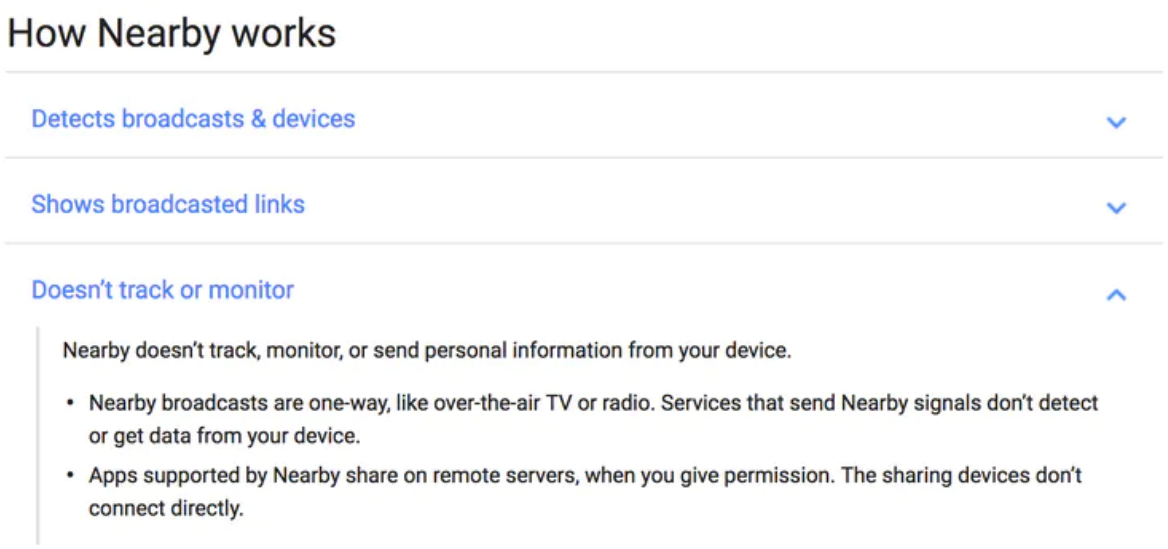
> *a device capable of being used to determine the geographical location of a person, vehicle or thing and any associated equipment.*

Since it is generally illegal to track someone without their consent – implied or otherwise – if an advertiser is using an app combined with an ultrasonic beacon to track you and you are unaware that they are doing so, they could be breaking the law.

Google says the Nearby protocol is battery-intensive due to the use of Bluetooth and wifi. As such "the user must provide consent for Nearby to utilise the required device resources". It says nothing about the legality of needing permission to record sound or track users.

Google does warn that the Nearby service is a one-way communication channel with your phone never communicating directly to a Nearby service on its online support page.

But since users are required to opt-out of the service, it's hard to argue that they have given informed consent.



Google explains that the Nearby devices do not connect directly as Lisnr technology does, however, nothing is specified about what happens to data from your phone to Google or other third-party servers.

What can I to protect my privacy?

Users need to be aware of the potential to be tracked from ultrasonic beacons such as Google's Nearby service.

Since this is a built-in feature of Google's Pixel phone and other Android phones, users need to have informed consent regarding the Nearby service and the dangers of revealing data about themselves. Merely blocking app permissions which request to use your phone's microphone will not be enough.

Read more: 7 in 10 smartphone apps share your data with third-party services

---

One research group has released a patch that proposes to modify the permission request on phones requiring apps to state when they want access to your microphone to track inaudible signals individually. This doesn't solve the built-in problem of Google's API though.

Google and other mobile phone companies should do more to ensure they are adequately gaining informed consent from users to ensure they do not fall foul of the law.

Thanks to reader feedback we've updated this article at the author's request to remove references to Apple's iBeacon, which does not use an acoustic side channel for data transfer.

Google **Apple** **Surveillance** **Regulation** **tracking** **Location data** **surveillance law**