The privacy problem with camera traps: you don't know who else could be watching

18 June 2018, by Paul D Meek, Greg Falzon And James Bishop

A spotted-tailed Quoll detected during a small mammal survey at Carrai Plateau, New South Wales. Credit: Paul Meek, Author provided

We use remotely activated cameras – known as camera traps – to study the ecology and population responses of wildlife and pest species in management programs across Australia.

These devices are used widely by scientists, researchers and managers to detect rare wildlife, monitor populations, study behaviour and measure long term wildlife population health.

But the lack of transparency surrounding how these images are transmitted, where they are stored, and who has access to them in transit, has scientists worried.

We've discovered that images captured by these devices may potentially be accessed by more than those intended, and that this could pose potential privacy breaches, and even poaching risks.

A chance discovery

It was an accidental discovery that our images can travel from the field to big overseas internet servers. We had not considered the transmission path of our images, and who may have access to them along the way.

Manufacturers have developed camera traps that are capable of transmitting image data using the telecommunications network (in Australia this is 3G and soon to move to 4G).

Most of these camera trap models can transmit images using both MMS (Multi Media Message Service), where the image is sent in an SMS (Short Message Service) to a smart phone, and via SMTP (Simple Mail Transfer Protocol), where the image is transmitted to an email address.

In Australia, when you buy a 3G compatible camera trap you just need to add a SIM card from a service provider. The images will then be sent from the camera trap at a field site to your work or home in seconds. This process is made simple for users by manufacturers who set up default settings to assist you in programming the camera trap.

A 3G camera trap set in the Strzelecki Desert and sending images to the authors email and phone. Credit: PM, Author provided

We have been testing and comparing several models of 3G camera trap, which includes evaluating the message structure and headers.

It was these investigations that revealed some alarming information that pose several potential risks to camera trap users when a camera trap is set up using the default settings for SMTP transmission.

Each manufacturer will use different methods, but in essence when an image is transferred through some 3G telecommunication service, the image is sent to one or more web-servers, where the image may be stored, then sent to the recipient email address or phone.

These servers can be in any country. Our investigations of the five models we tested identified that images are being sent via some large, well-known Asian and North American companies. The exact location of each server, and the full transmission pathway cannot be fully known.

Exactly what happens to these images during transmission also remains unknown. But most practitioners we have spoken to have no idea their images could potentially be going to servers overseas, so it raises several concerns for users.

If, like most people, you don't over-ride the default settings, then your data will be managed for you. An attractive offer, especially for those people who are not tech-savvy or who don't have time to fiddle around with programming equipment.

But where are your images going? Who has the legal right to access and store them? How secure is each stage of the transmission path, and are your images being used without your knowledge?

An evaluation process

Our research team has been evaluating the transmission of images via SMTP for a larger research project, aimed at developing camera trap transmission via satellite.

A harmless image of an un-suspecting person walking past a camera trap could end up in a court of law if the

image is used without their permission. Credit: Paul Meek, Author provided

The right thing captured in the camera trap: a spotted-tailed Quoll. Credit: Paul Meek, Author provided

A privacy concern

One of our foremost concerns is how legal professionals would interpret ownership and distribution of images of people under privacy legislation. Camera traps deployed to detect wildlife often detect unsuspecting people walking past.

It's a legal mine field when a camera trap user potentially distributes an image of a person without their permission.

It was an issue raised back in 2012 when an unnamed Austrian politician was caught in a sexual encounter by a camera trap. In that case the image wasn't released publicly but it raised concerns over a potential breach of privacy.

In Australia, such an image belongs to the person who is photographed irrespective of where the images were taken, so strictly speaking they could pursue legal action against anyone distributing it.

Clearly there would be extenuating circumstances, but whether or not there is a case to be answered is yet to be tested and would depend on the country and legislation involved.

Camera traps are also used for security purposes by authorities, farmers and members of the public, so potential legal and sensitive data could be distributed over the internet. As there is a lack of transparency surrounding the transmission pathway, storage, and usage of the data, this could be a huge concern.

In Australia, this might constitute a breach under the Privacy Act 1988 dependent on the whether any personal data is disclosed and the potential for serious harm which might result.

All in the cloud

The Australian government has released policy and guidelines concerning the protection of data privacy when using cloud services.

But these requirements might not extend, or have not been adopted, in the context of technological based ecology monitoring and so valuable data could currently be leaving Australian shores.

How this data is used is also largely unknown. It may serve many commercial purposes for companies, such as data mining, advertising, and machine learning and artificial intelligence development, to name but a few. Exactly what country, where and how securely the data is stored remains a mystery.

Of real concern for many international wildlife conservation groups is the potential misuse of wildlife images that could identify threatened species and locations. This information could be illegally accessed by poachers, or those looking to sell the data for profit.

Our disclaimer here is that we have no evidence to prove or deny that such practices are occurring, but the potential exists and the lack of transparency is

alarming.

Reducing the risk

Until recently we did not fully comprehend the risks we were taking by using 3G camera traps without taking some precautions. Like most, we accepted that our data was safe and controlled by Australian telecommunications systems, and had no concept that the images may be transmitted or stored by servers overseas.

We now know the risks and that in many cases this image management protocol can be circumvented by over-riding the camera's default settings. In the ideal world every user would know the full transmission pathway of the image and could take steps to make sure it is as secure as practically possible. Given this is not possible, we recommend that where possible, users program camera traps to send SMTP images direct to an email address that they have more control over.

It will take a little extra time to program the camera traps, but at least users will have more control over the path of their image from the field to any receiving device.

This article was originally published on The Conversation. Read the original article.