

New research reveals two-thirds of second-hand memory cards contain personal data from previous owners

June 29 2018



Credit: University of Hertfordshire

University of Hertfordshire research finds people aren't sufficiently erasing data before selling old memory cards from mobile phones, tablets and other connected devices.

New research finds that two-thirds of second-hand memory cards found in mobile phones or tablets and sold to the public still contain [personal data](#) from their previous owners. The study, commissioned by Comparitech.com—the security and privacy reviews and comparison website, analysed data held and therefore sold on used memory cards. This analysis uncovered a host of personal information and sensitive materials, including passport copies, contact lists and identification numbers being passed from one person to the next.

The team at the University of Hertfordshire purchased and analysed 100 used SD and micro SD memory cards from eBay, conventional auctions, second-hand shops, and other sources over a four-month period. They created a forensic image, a bit-by-bit copy, of each card, then used freely available software to recover data. The majority of cards were used in smartphones and tablets, while other devices also included cameras, SatNav systems, and even drones.

Data recovered from the used memory cards worryingly included [personal information](#) and sensitive materials such as intimate photos and selfies, passport copies, contact lists, navigation files, pornography, resumes, browsing history, identification numbers and other important personal documents.

Professor Andrew Jones, Professor of Cyber Security at the University of Hertfordshire said: 'This research uncovers the prevalence of second-hand memory cards providing a rich source of sensitive data, that could easily be misused if a buyer so wished. Despite the ongoing media focus on cybercrime and the security of personal data, it is clear from our research that the majority are still not taking adequate steps to remove all data from [memory cards](#) before sales.

'Particularly important is satellite navigation systems (SatNav) data, which can be used to determine the home location of the user, and also

the routes that they regularly use and locations that they have identified as being of interest, which may include their place of work and the homes of family and friends. Again, this information in the wrong hands could easily put previous owners at risk.

'At the University of Hertfordshire's Cyber Security Centre, we are focused on investigating and developing tools and techniques capable of detecting and responding to a variety of cyber based attacks, including the collection of digital forensic evidence.'

Paul Bischoff, Privacy Advocate for Comparitech.com said: "As exemplified in this report, often the problem is not that people don't wipe their SD cards; it's that they don't do it properly. Simply deleting a file from a device only removes the reference that points to where a computer could find that file in the card memory. It doesn't actually delete the ones and zeros that make up the file. That data remains on the card until it is overwritten by something else. For this reason, it's not enough to just highlight all the files in a memory card and hit the delete key. Retired cards need to be fully erased and reformatted.

'From posting intimate pictures on the web without their knowledge that could be subject to facial recognition technology, illegitimate use of children's photos that may be stored on these [memory](#) card; or using or selling ID documents like a passport to commit fraud – the outcomes are truly scary.'

The full breakdown from the 100 cards studied is as follows:

- 36 were not wiped at all, neither the original owner nor the seller took any steps to remove the data.
- 29 appeared to have been formatted, but data could still be recovered "with minimal effort."
- 2 cards had their data deleted, but it was easily recoverable

- 25 appeared to have been properly wiped using a data erasing tool that overwrites the storage area, so nothing could be recovered.
- 4 could not be accessed (read: were broken).
- 4 had no [data](#) present, but the reason could not be determined

There's more information on the topic on [Comparitech.com's website](#).

Provided by University of Hertfordshire

Citation: New research reveals two-thirds of second-hand memory cards contain personal data from previous owners (2018, June 29) retrieved 13 July 2024 from <https://phys.org/news/2018-06-reveals-two-thirds-second-hand-memory-cards.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.