Smart Devices & Secure Data Eradication: the Evidence
Aim of the Research

To assess the scale of the data eradication issue now and in the future and identify threats and risks that could discourage consumers from reusing or recycling smart devices.

The evidence

The range of smart devices is expanding rapidly and increasingly collect and store personal information. While WRAP advocates for consumers to reuse these more often, the ability to eradicate the data at end of life is essential. A known barrier to the reuse of these smart gadgets is the inability to eradicate data from them.

WRAP commissioned Giraffe Innovation Ltd to undertake this research to:

- Gather evidence on the size of the data eradication issue in end-of-life Electrical and Electronic Equipment (EEE) between 2012 up to 2020; and
- Identify actions that WRAP Electrical and Electronic Equipment Sustainability Action Plan (esap) signatories and other key stakeholders can take to encourage appropriate reuse or recycling of smart devices.

The methodology included literature review, modelling, stakeholder survey and workshop.
Secure Data Eradication: The Issue Now

Research and case studies via literature review did show restoring the factory setting in the menu system, physical hard drive, memory card or operating system is not an effective way of eradicating personal data that was meant to be deleted or destroyed.

Example: Smartphones.
50% password encrypted and 90% passcode locked;
• Owners’ e-mail addresses were recovered in 90%;
• Owner identified in 75%;
• Contacts recovered in 75% of cases; and
• Browsing history in 75% of cases.

Smartphones that had been ‘factory wiped’:
• Text/chat logs was recovered (85%);
• Contacts details (60%); and
• Owners’ e-mail address identified in 60%.

(Source: Deloitte, 2014)

Example: 200 hard drives and memory sticks
Bought from online internet auction sites and computer trade fairs. Over 34,000 residual files found including:
• Scanned bank statements;
• Passports; and
• Medical details.

(Source: The ICO/NCC Group, 2010)

Example: Random sample of Hard and Solid Disk Drives recovered from 10 manufacturers found:
• Devices being resold without any deletion method applied in 25%;
• Devices (75%) had a deletion attempt including ‘quick formatted and formatted, basic delete, random ‘over write’ and reinstalled software prior to resale; and

All of the data (444,000 files) above were retrieved as only a basic delete or sent to the recycle bin had been performed.

(Source: Blancco and Kroll Ontrack, 2015)
The evidence aforementioned highlights limited consumer knowledge on how to securely wipe data from smart devices prior to disposal, trade-in and resale.

Consumer awareness and therefore attitudes and behaviour play an important part in the data eradication issue.

Key specific problems include:
- Lack of knowledge of the risks of personal data left on devices;
- Lack of awareness that there is any personal data left on devices;
- Lack of knowledge of options for data eradication and whether adequate; and
- Lack of knowledge of which devices present a risk.
Other consumer issues identified include hoarding, where concerns around personal data security have discouraged 35% of UK households from disposing of a product, resulting in the hoarding.

- Households (61%) have at least one smart device stored and unused at home;
- Up to 125 million mobile phones may already be hoarded in the UK.

(Source: WRAP's Sustainable EEE Consumer Tracker - Survey of 2,186 people - Spring 2016)
Consumer actions to eradicate data from devices

A number of factors are deduced which include:

- Limited information from the producer or operating system supplier;
- Lack of awareness that deleting files and formatting the hard drive does not fully eradicate the data;
- Lacking information on available data eradication software;
- Assuming that resetting to factory defaults eradicates the data; and
- A perception that removing the hard drive from the device and disposing of it separately makes the data unreadable.
The Numbers: UK Household ownership of 17 Smart Devices

The modelling used market sales data to account for predicted changes in sales volumes across the WEEE categories. WRAP's 'Market flows of WEEE materials' (Weibull analysis of product lifetimes) was used to calculate numbers of smart devices arising as WEEE and volumes offered for reuse from 2016 to 2020.

UK household ownership across 17 smart product categories (OECD, 2014) is forecast at 272 million devices by 2017 (10 per household) and 423 million by 2020 (15 per household). Smart devices containing data entering the waste stream will be 40 million in 2016, rising to 81 million in 2020, with an estimated 2.5 million items offered for reuse in 2016, rising to 4.2 million in 2020. This is on average 6.5% of the total products reaching the end of life (EOL) with over 90% of these presenting a ‘high’ data security risk as they could contain sensitive data on operating systems, hard drives and memory.

17 Smart Devices Product Categories

1. Smartphones;
2. Tablets;
3. Laptops;
4. E-readers;
5. Personal computers (PCs);
6. Smart watches;
7. Smart set top boxes
8. Games consoles;
9. Smart Televisions;
10. Smart washing machines;
11. Smart Fridges;
12. Health and fitness monitors;
13. Smart sports devices;
14. Smart stereos;
15. Smart digital cameras;
16. Home automation sensors; and
17. Smart lighting.
Increased ownership of smart devices

For the 17 product categories included in this study UK households ownership of all smart devices (OECD, 2014) is estimated at 272 million devices in 2017 (10 per household) and 423 million in 2020 (15 per household). Smartphones are predicted as the most common item owned, accounting for 19% of smart devices in 2017 (65 million items), increasing to 67 million Smartphones owned by households in 2020.
Resale of ‘High Risk’ smart devices

Ten products present a higher data eradication risk and typically contain hard drives, memory cards and internet access where the user will have inputted sensitive data.

These have high sales volumes and WEEE arising and account for 2.52 million of the 2.55 million devices being offered for resale in 2016 (99%) and 3.99 million of the 4.2 million in 2020 (95%) (Internet Advertising Bureau for the UK, 2015).

The smartphone in particular confirms the current and expected trend of the industry steady growth both in market size as well as new opportunities to use mobile technology such as mobile payments. Data eradication issue will therefore be critical as more people start using their smartphones for mobile commerce.
This research identifies 4% of the high risk EOL smart devices, (1.5 million in 2016 to over 2.7 million in 2020), would have had nothing done to them to eradicate the data before being passed on for recycling or reuse.

### Numbers of smart devices containing unadulterated data

<table>
<thead>
<tr>
<th>Smart device</th>
<th>2016 (million units)</th>
<th>2020 (million units)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphones</td>
<td>0.657</td>
<td>1.07</td>
</tr>
<tr>
<td>Tablets</td>
<td>0.305</td>
<td>0.610</td>
</tr>
<tr>
<td>Laptops</td>
<td>0.180</td>
<td>0.167</td>
</tr>
<tr>
<td>E-readers</td>
<td>0.001</td>
<td>0.005</td>
</tr>
<tr>
<td>PCs</td>
<td>0.260</td>
<td>0.02</td>
</tr>
<tr>
<td>Smart watches</td>
<td>0.001</td>
<td>0.051</td>
</tr>
<tr>
<td>Set top boxes</td>
<td>0.014</td>
<td>0.188</td>
</tr>
<tr>
<td>Games consoles</td>
<td>0.069</td>
<td>0.089</td>
</tr>
<tr>
<td>Smart TVs</td>
<td>0.019</td>
<td>0.307</td>
</tr>
<tr>
<td>Total</td>
<td><strong>1.506</strong></td>
<td><strong>2.689</strong></td>
</tr>
</tbody>
</table>

### Example: Smartphones end of life and reuse

16.4 million smartphones will reach their end of life in 2016 rising to over 26 million in 2020. Of these 1.15 million are expected to be reused in 2016 and 1.9 million in 2020. (Internet Advertising Bureau for the UK, 2015)
Stakeholder Survey: IT Asset Management (ITAM) Company Research

A questionnaire was distributed* to ITAMs reprocessing smart devices in order to understand current data eradication practices and issues.

All respondents offered a data eradication service to businesses for smartphones and tablets with 8 offering a data eradication service that also included laptops and PCs. However, only 4 ITAMs offered a similar service to consumers. The survey revealed:

- Established accredited data eradication services and certified techniques in the business to business (B2B) market. This is offered by ITAMs primarily for the disposal, recycling and resale of smartphones, tablets and laptops; and
- Lack of industry standards for data eradication for items such as smart TVs, white goods, smart hi-fi, smart watches.

Data eradication carried out by ITAMs is undertaken to levels specified by legislation, organisations or standards including:

- GDPR – General Data Protection Regulation;
- The UK Data Protection Act;
- CESG (to be replaced by the National Cyber Security Centre in October 2016) HMG IA Standard No. 5;
- NIST_800-88;
- ADISA;
- EN15713 ‘Secure Destruction of Confidential Material’;
- CPNI – Centre for the Protection of National Infrastructure;
- ISO/IEC 27001:2013 - information security standard for an information security management system (ISMS);
- PAS 7010: 2016 Secure destruction of sensitive material;
- The PCI Security Standards (PCISS); and
- BS EN 50614 Requirements for the preparation for reuse of waste electrical and electronic equipment.

* 9 Companies responded from 35 ADISA members and WRAP’s esap signatories.
Stakeholder Engagement Workshop

A workshop with industry and Government stakeholders highlighted the wide range of stakeholders affected by the data eradication issue. Most who have not yet understood the potential implications of the subject particularly brand and original equipment manufacturers (OEM), retailers and consumers. The focus of the discussion was on risks, opportunities, actions that can be taken by key stakeholders.

A consistent theme from the stakeholders was that although there are a wide range of standards and advice available there is need for:

- A detailed and coherent guidance for stakeholders on their liabilities and protocols for data eradication; and
- A simple advice to consumers on how to eradicate data on their device(s) as well as awareness when selecting a professional data eradication service provider at end of life.

New : General Data Protection Regulation (GDPR)

The stakeholders identified new regulation GDPR proposed to replace the Data Protection Act could have had a significant impact on the sector and their responsibilities.

Although scheduled to come into force on 25 May 2018, the uncertainty of the outcome of UK negotiations on the terms of its exit from the EU brings into question whether or for how long the Regulation will directly apply in the UK.

A statement by a spokesperson for the Information Commissioner’s Office (ICO) on 27 Jun 2016 via outlaw.com confirmed that:

“The Data Protection Act "remains the law of the land" at the moment. The UK data protection reforms are "necessary" and that the data protection framework in the UK would need to accord to the standards outlined in the GDPR if the UK wishes to "trade with the [EU] single market on equal terms" in the event that the Regulation does not "directly apply to the UK".
New: General Data Protection Regulation (GDPR)

With the above mentioned GDPR could ‘change the regulatory landscape’ and could affect any company that collect, store and use customer data.

Key relevant specifics include:

• Impose a right to have personal data erased ‘without undue delay’ under certain circumstances;
• ‘Privacy by Design and by Default’ - require that data protection is designed into the development of business processes for products and services; and
• The maximum fines for noncompliance will be set at 4% of an organisation’s worldwide turnover, or €20 million, whichever is higher – per incidence.

It is recognised that with so many original equipment manufacturers (OEM), retailers and consumers operating across borders, consistency around data protection laws and rights is crucial. Clear laws with safeguards in place are more important than ever in the growing digital economy. The ICO's role has always worked closely with regulators (domestic and abroad), and it is likely continue to do so regardless of the position of the UK's membership in the EU.
Conclusions

The research has highlighted the increased range and volumes of smart devices available on the market up to 2020 along with the current data eradication risks associated with these devices.

Based on all of the analysis conducted for this project, the following key conclusions have been made.

The household market for smart devices is likely to continue to grow rapidly over the next five years and the UK will have an estimated 13% of the European market based upon GDP. 90% of the total products reaching present a ‘high’ data security risk.

Smart devices will increasingly collect and store more personal information as they interact with each other and owners’ smart devices.

There is limited reliable information for consumers on how to eradicate data and reassurance that their data will be handled securely after disposal, trade-in or sale.

There are a wide range of stakeholders affected by the data eradication issue, as well as those who have not yet understood the potential implications of the subject. This includes:

- Manufacturers and Brands;
- Retailers;
- Local authorities;
- Waste management companies;
- Reuse organisations (including charities);
- Producer compliance schemes (PCSs);
- IT Asset Management companies (ITAMs); and
- Householders.

The new GDPR has changed the regulatory landscape with significant requirements for key stakeholders to follow or they will be clearly identified as being in direct contravention of the regulation.

Accredited data eradication services and certified techniques are established in the B2B market offered by ITAMs primarily for the disposal, recycling and resale of smartphones, tablets and laptops.
## Recommendations for actions by key stakeholders with support from WRAP

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Risk</th>
<th>Opportunities</th>
<th>Action(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumers</td>
<td>Limited and reliable information available on how to eradicate data.</td>
<td>Broadening of knowledge on data eradication issue (the why and how).</td>
<td>Dedicated consumer research to understand concerns regarding data on smart devices and the effect this has on the sale, disposal or donation of these devices.</td>
</tr>
<tr>
<td>Manufacturers and brands</td>
<td>Data protection regulations/reforms - obligation to ensure that privacy is embedded into any new processing or product deployed.</td>
<td>A leadership role in building consumer trust in smart devices and secure data eradication processes via product design, dedicated software for secure data eradication and communication activities etc.</td>
<td>Provision of enabling tools for consumer data eradication. Communication campaign on best practice in secure data bearing devices. Further assessment of potential risk and compliance with data protection regulations/reforms.</td>
</tr>
<tr>
<td>ITAMS</td>
<td>Compliance under relevant regulations on minimum requirements for the safe treatment, recycling and secure data eradication.</td>
<td>Offer a consumer facing data eradication service for smart devices.</td>
<td>Work with producers and retailers to increase consumer awareness on how to securely dispose or eradicate data from smart devices.</td>
</tr>
<tr>
<td>Retailers</td>
<td>Liabilities under any new Data Protection Regulations/reforms.</td>
<td>Offer a lower financial rebate to consumers for trade-in with peace of mind on secure data eradication. This has the potential to increase market penetration of the service.</td>
<td>Research on what retailers currently communicate regarding the need for data eradication.</td>
</tr>
</tbody>
</table>
## Recommendations for actions by key stakeholders with support from WRAP

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Risk</th>
<th>Opportunities</th>
<th>Action(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Producer compliance schemes (PCS)</td>
<td>Duty of Care to ensure that any waste recyclers handling data bearing devices eradicates the data to an acceptable standard. The risk of smart devices being stolen from poorly protected and monitored HWRC.</td>
<td>Raise the awareness of data eradication issues including product hoarding limiting disposal and consequently WEEE collection.</td>
<td>Communicate data security and relevant regulations to their members. Encourage producers to work collaboratively on awareness building campaign.</td>
</tr>
<tr>
<td>Household Waste Recycling Centre (HWRC)</td>
<td>Duty of Care to ensure that waste contractors handling data bearing devices on its behalf, eradicates the data to an acceptable standard. The risk of smart devices being stolen from poorly protected and monitored HWRC.</td>
<td>Ensure that the appropriate data security protocols are in place with the waste contractors for data bearing devices collected from these sites. The need to increase awareness of consequences and liabilities related to smart devices being stolen from HWRC. Increase security.</td>
<td>Promote and raise awareness of the issue of data security and eradication. Information about data eradication within the disposal, recycling and reuse process could re-inforce positive messaging for consumers and increase WEEE take-back.</td>
</tr>
<tr>
<td>LAs</td>
<td>Duty of Care via contracts with the operators of HWRC.</td>
<td>Facilitate robust protocols and traceability of data bearing devices and treatment at HWRC and Approved Authorised Treatment Facilities (AATFs).</td>
<td>Increase awareness of data eradication within LAs and HWRCs as well as their contractors.</td>
</tr>
<tr>
<td>UK Government</td>
<td>N/A</td>
<td>Extend the work and communications to businesses on data security to include end of life products.</td>
<td>Explore opportunities to address data security issues through to end of life data eradication on products.</td>
</tr>
<tr>
<td>Information Commissioner’s Office (ICO)</td>
<td>N/A</td>
<td>Extend the work on data security to end of life products.</td>
<td>Enhance the basic information on data eradication available from the ICO plus, national cyber security centre to demonstrate data eradication risks and opportunities.</td>
</tr>
</tbody>
</table>
Manufacturers and retailers of smart devices are considered as the most powerful actors for next steps in the data eradication issue. Brands with their influence on product design and retailers with their consumer facing position are well situated to take a leadership position in addressing consumer concerns on the data eradication issue. Leadership from manufacturers and retailers is therefore considered critical to ensure that EOL products are properly managed in light of data eradication risk. Their potential actions could include but are not limited to:

- Provide inbuilt functionality or software allowing eradication of data from the product – ‘secure by design’;
- Integrate communication awareness on how to safely eradicate data on smart devices prior to disposal;
- Undertake research to understand gaps in smart device manufacturer’s protocols on data eradication and a technical assessment of their efficacy; and
- Undertake an assessment of potential risk and compliance with GDPR Regulations for key stakeholders in this sector.

Further research could include:
- Understanding concerns consumers have about the potential for data left on smart devices and the effect this has on the sale, disposal or donating of devices; and
- How retailers and take back organisations are advertising services and information on data eradication both now and in the future.
WRAP’s Vision
Our Vision is a world where resources are used sustainably. It works in partnership with governments, businesses, trade bodies, local authorities, communities and individuals looking for practical advice to improve resource efficiency that delivers both economic and environmental benefits.

WRAP’s Mission
Our Mission is to accelerate the move to a sustainable resource-efficient economy through:

- **re-inventing** how we design, produce and sell products;
- **re-thinking** how we use and consume products; and
- **re-defining** what is possible through re-use and recycling.

Disclaimer
While we have tried to make sure this report is accurate, WRAP does not accept liability for any loss, damage, cost or expense incurred or arising from reliance on this report. Readers are responsible for assessing the accuracy and conclusions of the content of this case study. Quotations and case studies have been drawn from the public domain, with permissions sought where practicable. This report does not represent endorsement of the examples used and has not been endorsed by the organisations and individuals featured within it. This material is subject to copyright. You can copy it free of charge and may use excerpts from it provided they are not used in a misleading context and you must identify the source of the material and acknowledge WRAP’s copyright. You must not use this report or material from it to endorse or suggest WRAP has endorsed a commercial product or service. For more details please see WRAP’s terms and conditions on our website at www.wrap.org.uk