hacker
A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term. See also: cracker.

cracker
A cracker is an individual who attempts to access computer systems without authorization. These individuals are often malicious, as opposed to hackers, and have many means at their disposal for breaking into a system. See also: hacker, Computer Emergency Response Team, Trojan Horse, virus, worm.
Steve Burrows FRSA CDir FIoD CITP FBCS

Over 40 years experience messing with computers and programming
35 years earning my living in “Information Technology”
Fellow of BCS The Chartered Institute for IT & Chartered IT Professional

Hardware Design, Software Development, Database Administration, Networking, Telecomms, Cyber Security, Reverse Engineering, Information Engineering, Informatics, Data Science, IT Leadership & Management

Chief Information Officer / “Hacker”
SRR Upsides

Cheaper - automatically ensure Resident ID / Address data is entered / updated across all relevant Gov’t databases

More accurate - reduce Gov’t cost to taxpayer by reducing Gov’t identification & addressing errors / resident ID queries - saves time and bureaucracy

Improved data protection compliance - Gov’t has a statutory duty to ensure that personal data it holds is accurate and up to date

Better demographic information for policy making - bulk analysis could enable development of more evidence-based policies and services displacing ideological, cultural and political biases

More joined-up - easier / simpler for different Gov’t service / benefits providers to ensure that individual residents receive more of the services / benefits to which they are entitled with fewer questions
SRR How?

SRR or Distributed Database Update:

Single Resident Record = a Master / Index Database - used to update or be the central reference point for all other databases

Distributed Database Update = a software mechanism to change all relevant databases when you update your details

The mechanism makes no odds, whichever way a universal update is achieved it implies a key field or composite key (combination of fields) which uniquely identifies the resident in each Gov’t database to locate and update their data.
**SRR Downsides**

Eggs in one basket - necessarily the creation of a mechanism which can update all Gov’t databases implies the ability to interrogate the same databases

Hacking - by malicious actors to acquire residents sensitive personal data

Abuse - by IoMG workers using legitimate access for illegitimate purposes

Political - numerous social / welfare / employment strategies and policies could be undermined by objective / factual data

Manipulation - data, like statistics, are subject to qualification and interpretation. Very difficult to ensure “single version of truth”
Gov't Cyber Sec Will Keep Data Safe?

No.


US, UK, Australian, Chilean, Greek, Norwegian, South African Gov’ts amongst biggest known data breaches.

<table>
<thead>
<tr>
<th>Organization/Event</th>
<th>Year</th>
<th>Number of Records</th>
<th>Sector</th>
<th>Type of Data Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Immigration Department</td>
<td>2015</td>
<td>G20 world leaders</td>
<td>government</td>
<td>accidentally published</td>
</tr>
<tr>
<td>California Department of Child Support Services</td>
<td>2012</td>
<td>800,000</td>
<td>government</td>
<td>lost / stolen media</td>
</tr>
<tr>
<td>City and Hackney Teaching Primary Care Trust</td>
<td>2007</td>
<td>160,000</td>
<td>government</td>
<td>lost / stolen media</td>
</tr>
<tr>
<td>Commission on Elections</td>
<td>2016</td>
<td>55,000,000</td>
<td>government</td>
<td>hacked</td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td>2016</td>
<td>30,000</td>
<td>government</td>
<td>poor security</td>
</tr>
<tr>
<td>Driving Standards Agency</td>
<td>2007</td>
<td>3,000,000</td>
<td>government</td>
<td>lost / stolen media</td>
</tr>
<tr>
<td>Embassy Cables</td>
<td>2010</td>
<td>251,000</td>
<td>government</td>
<td>inside job</td>
</tr>
<tr>
<td>Florida Department of Juvenile Justice</td>
<td>2013</td>
<td>100,000</td>
<td>government</td>
<td>lost / stolen computer</td>
</tr>
<tr>
<td>Greek government</td>
<td>2012</td>
<td>9,000,000</td>
<td>government</td>
<td>hacked</td>
</tr>
<tr>
<td>Jefferson County, West Virginia</td>
<td>2008</td>
<td>1,000,000</td>
<td>government</td>
<td>accidentally published</td>
</tr>
<tr>
<td>Massachusetts Government</td>
<td>2011</td>
<td>210,000</td>
<td>government</td>
<td>poor security</td>
</tr>
<tr>
<td>Ministry of Education (Chile)</td>
<td>2008</td>
<td>6,000,000</td>
<td>government</td>
<td>accidentally published</td>
</tr>
<tr>
<td>Norwegian Tax Administration</td>
<td>2008</td>
<td>3,950,000</td>
<td>government</td>
<td>accidentally published</td>
</tr>
<tr>
<td>Office of Personnel Management</td>
<td>2015</td>
<td>21,500,000</td>
<td>government</td>
<td>hacked</td>
</tr>
<tr>
<td>Office of the Texas Attorney General</td>
<td>2012</td>
<td>6,500,000</td>
<td>government</td>
<td>accidentally published</td>
</tr>
<tr>
<td>Oregon Department of Transportation</td>
<td>2011</td>
<td>unknown</td>
<td>government</td>
<td>poor security</td>
</tr>
<tr>
<td>San Francisco Public Utilities Commission</td>
<td>2011</td>
<td>180,000</td>
<td>government</td>
<td>hacked</td>
</tr>
<tr>
<td>Service Personnel and Veterans Agency (UK)</td>
<td>2008</td>
<td>50,500</td>
<td>government</td>
<td>lost / stolen media</td>
</tr>
<tr>
<td>South Africa police</td>
<td>2013</td>
<td>16,000</td>
<td>government</td>
<td>hacked</td>
</tr>
<tr>
<td>State of Texas</td>
<td>2011</td>
<td>3,500,000</td>
<td>government</td>
<td>accidentally published</td>
</tr>
<tr>
<td>Syrian government (Syria Files)</td>
<td>2012</td>
<td>2,434,899</td>
<td>government</td>
<td>hacked</td>
</tr>
<tr>
<td>Texas Lottery</td>
<td>2007</td>
<td>89,000</td>
<td>government</td>
<td>inside job</td>
</tr>
<tr>
<td>UK Home Office</td>
<td>2008</td>
<td>84,000</td>
<td>government</td>
<td>lost / stolen media</td>
</tr>
<tr>
<td>UK Ministry of Defence</td>
<td>2008</td>
<td>1,700,000</td>
<td>government</td>
<td>lost / stolen media</td>
</tr>
<tr>
<td>UK Revenue &amp; Customs</td>
<td>2007</td>
<td>25,000,000</td>
<td>government</td>
<td>lost / stolen media</td>
</tr>
<tr>
<td>U.S. Army (classified Iraq War documents)</td>
<td>2010</td>
<td>392,000</td>
<td>government</td>
<td>inside job</td>
</tr>
<tr>
<td>U.S. law enforcement (70 different agencies)</td>
<td>2011</td>
<td>123,481</td>
<td>government</td>
<td>accidentally published</td>
</tr>
<tr>
<td>Washington State court system</td>
<td>2013</td>
<td>160,000</td>
<td>government</td>
<td>hacked</td>
</tr>
<tr>
<td>Medicaid</td>
<td>2012</td>
<td>780,000</td>
<td>government, healthcare</td>
<td>hacked</td>
</tr>
<tr>
<td>Virginia Department of Health</td>
<td>2009</td>
<td>8,257,378</td>
<td>government, healthcare</td>
<td>hacked</td>
</tr>
<tr>
<td>U.S. Department of Veteran Affairs</td>
<td>2008</td>
<td>26,500,000</td>
<td>government, military</td>
<td>lost / stolen computer</td>
</tr>
</tbody>
</table>
“Hacker” discloses how he accidentally discovered ways to view or change anyone’s UK HMRC tax records via HMRC public web portal due to poor programming.

And how it took 57 days to get HMRC to accept the problems and fix them. 

*(but only by threatening to go public)*
Gov’t Staff Can Be Trusted With Data?

No.

Even in MI5 and GCHQ where data access is rigorously controlled and logged, personal data abuse is rife.

IoM Gov’t is no different - it is made up of people like us, some good, some not so good.
Gov’t Can Be Trusted With Data?

No.

Governments have been repeatedly guilty of abusing citizens data privacy.

We can trace European data protection law back to the crimes of the Nazis. In the late 1950’s Germans started to seek protection from state processing of personal data about race, religion, employment, income, political allegiances etc.

The world’s first data protection act was adopted in the German state of Hessen in 1970; and the German Federal Data Protection Act applying to all of “West” Germany was passed in 1977. COE Treaty 108 was ratified by most EEC countries in 1981 and came into effect in 1985. The UK Data Protection Act 1984 was passed to achieve compliance with COE Treaty 108.
Us and Them

Government cannot guarantee security from hacking

Government workers cannot all be trusted with our data

Government as an institution cannot be trusted with our data

The foundation of EC Data Protection law was to protect citizens from Government abuse of data

Most exemptions to existing National Data Protection laws are for the benefit of Governments

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

http://www.eugdpr.org/
Do We Have A Choice?

Not really. This is the 21st Century, the “Information Age”.

Proper use of citizens data to create information for policy development and economical delivery of services is Essential to create affordable public services “Proper” must be defined in law and independently supervised and enforced

Improper use of citizens data must be penalised to the maximum extent

We have to change Gov’t culture to inhibit personal data crime and enable the advantages of information in mitigating the increasing costs of public services
What Does The UK Gov’t Say?

Information sharing code of practice: public service delivery, debt and fraud
Published 21 September 2017

1.2 Principles for data sharing

- 12. It is of vital importance that data is handled in a way that inspires the trust and confidence of citizens. The following principles support the security of data and privacy of citizens whilst enabling the delivery of better services and outcomes for citizens and government.

- Data sharing agreements should, subject to limited exceptions, ensure that where datasets are linked, it should be for the specified purpose and *should not lead to the creation of new identity registers*. 
What Does The UK Gov’t Do?

It’s still happening.

Government abuses personal data - inc. IoMG.

It won’t change unless we make it change.
Current IoM Data Protection Penalties

General provisions relating to offences

55. Prosecutions and penalties

P1998/29/60

(1) No proceedings for an offence under this Act shall be instituted except by the Supervisor or by or with the consent of the Attorney General.

(2) A person guilty of an offence under any provision of this Act other than paragraph 12 of Schedule 8 is liable —

UK DPA 1998 - £500,000 fine

IoM DPA 2002 - £5,000 fine

Almost Zero disincentive to IoMG

Data Protection Act 2002

(a) on summary conviction, to a fine not exceeding £5,000, or
(b) on conviction on information, to a fine.
(3) A person guilty of an offence under paragraph 12 of Schedule 8 is liable on summary conviction to a fine not exceeding £5,000.
Changing Gov’t Culture on Data Crime

Current IoM Data Protection penalties are trivial and academic - no material inhibitor to Gov’t abuse of our data.

Tynwald must change the laws to enable the Single Resident Record, Inter-departmental Data Sharing, and Single Legal Entity.

In return for gifting the benefits of a Single Resident Record we should also change our laws so that penalties for Gov’t abuse of citizen data are material:

**Minimum mandatory 5 year imprisonment of Gov’t worker(s), and their Departmental CEOs and Ministers, for each and any abuse of citizen data.**
IoM Can Lead The World

IoM Gov’t Can and Does compel residents to hand over our personal data. Government is different to business, businesses cannot compel us. With Power must come Responsibility and Accountability.

SRR and all future IoM data law should recognise that a Gov’t-perpetrated data crime against one of us is as serious as a data crime against all c. 84,000 of us.

We should approve the “Single Resident Record”, we need it. We should require to approve each specific Purpose for use of our data. We should have zero tolerance for Government misuse of our data.