Positive Action Group Single Resident Record

Steve Burrows

RFC 1983: Internet Users' Glossary

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

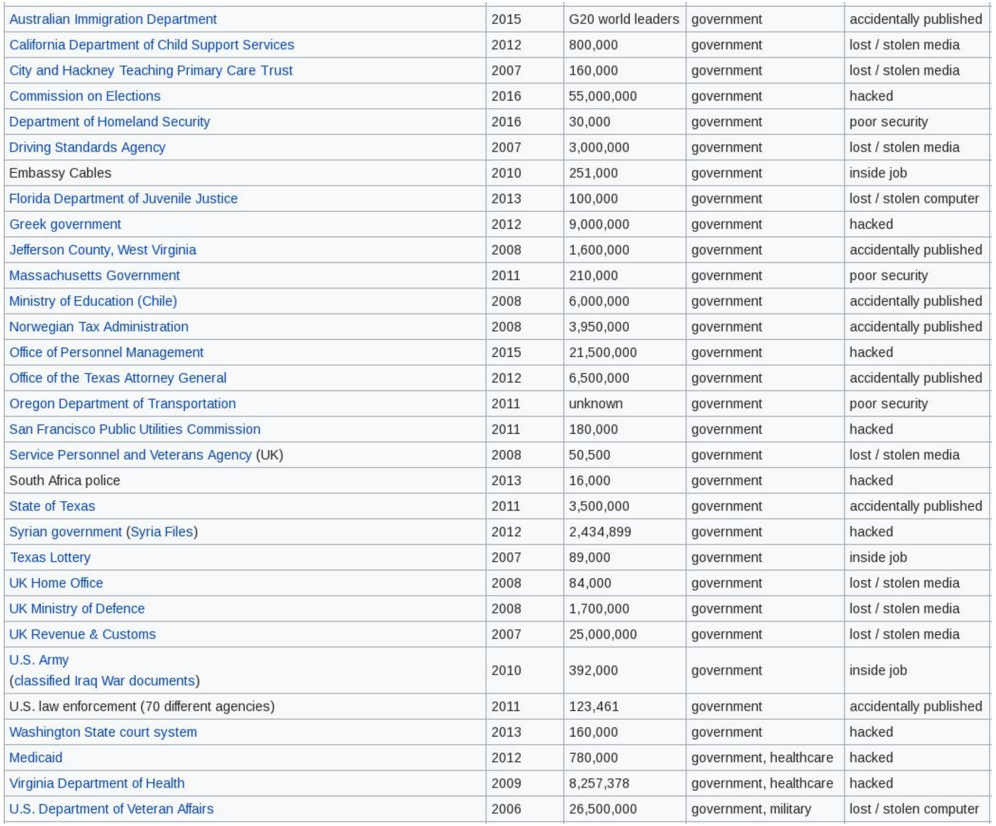
Hacking - by malicious actors to acquire residents sensitive personal data

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?



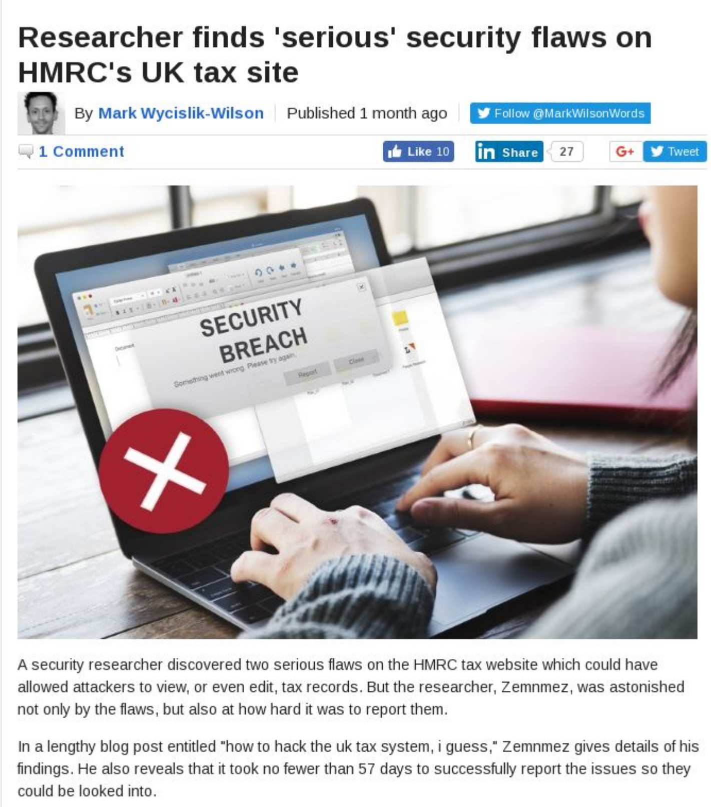
Australian Immigration Department	2015	G20 world leaders	government	accidentally published
California Department of Child Support Services	2012	800,000	government	lost / stolen media
City and Hackney Teaching Primary Care Trust	2007	160,000	government	lost / stolen media
Commission on Elections	2016	55,000,000	government	hacked
Department of Homeland Security	2016	30,000	government	poor security
Driving Standards Agency	2007	3,000,000	government	lost / stolen media
Embassy Cables	2010	251,000	government	inside job
Florida Department of Juvenile Justice	2013	100,000	government	lost / stolen computer
Greek government	2012	9,000,000	government	hacked
Jefferson County, West Virginia	2008	1,600,000	government	accidentally published
Massachusetts Government	2011	210,000	government	poor security
Ministry of Education (Chile)	2008	6,000,000	government	accidentally published
Norwegian Tax Administration	2008	3,950,000	government	accidentally published
Office of Personnel Management	2015	21,500,000	government	hacked
Office of the Texas Attorney General	2012	6,500,000	government	accidentally published
Oregon Department of Transportation	2011	unknown	government	poor security
San Francisco Public Utilities Commission	2011	180,000	government	hacked
Service Personnel and Veterans Agency (UK)	2008	50,500	government	lost / stolen media
South Africa police	2013	16,000	government	hacked
State of Texas	2011	3,500,000	government	accidentally published
Syrian government (Syria Files)	2012	2,434,899	government	hacked
Texas Lottery	2007	89,000	government	inside job
UK Home Office	2008	84,000	government	lost / stolen media
UK Ministry of Defence	2008	1,700,000	government	lost / stolen media
UK Revenue & Customs	2007	25,000,000	government	lost / stolen media
U.S. Army (classified Iraq War documents)	2010	392,000	government	inside job
U.S. law enforcement (70 different agencies)	2011	123,461	government	accidentally published
Washington State court system	2013	160,000	government	hacked
Medicaid	2012	780,000	government, healthcare	hacked
Virginia Department of Health	2009	8,257,378	government, healthcare	hacked
U.S. Department of Veteran Affairs	2006	26,500,000	government, military	lost / stolen computer

No.

https://en.wikipedia.org/wiki/List_of_data_breaches

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

ALL IT Systems 'R' Vulnerable



Researcher finds 'serious' security flaws on HMRC's UK tax site

By Mark Wycislik-Wilson | Published 1 month ago

1 Comment

A security researcher discovered two serious flaws on the HMRC tax website which could have allowed attackers to view, or even edit, tax records. But the researcher, Zemnmez, was astonished not only by the flaws, but also at how hard it was to report them.

In a lengthy blog post entitled "how to hack the uk tax system, i guess," Zemnmez gives details of his findings. He also reveals that it took no fewer than 57 days to successfully report the issues so they could be looked into.

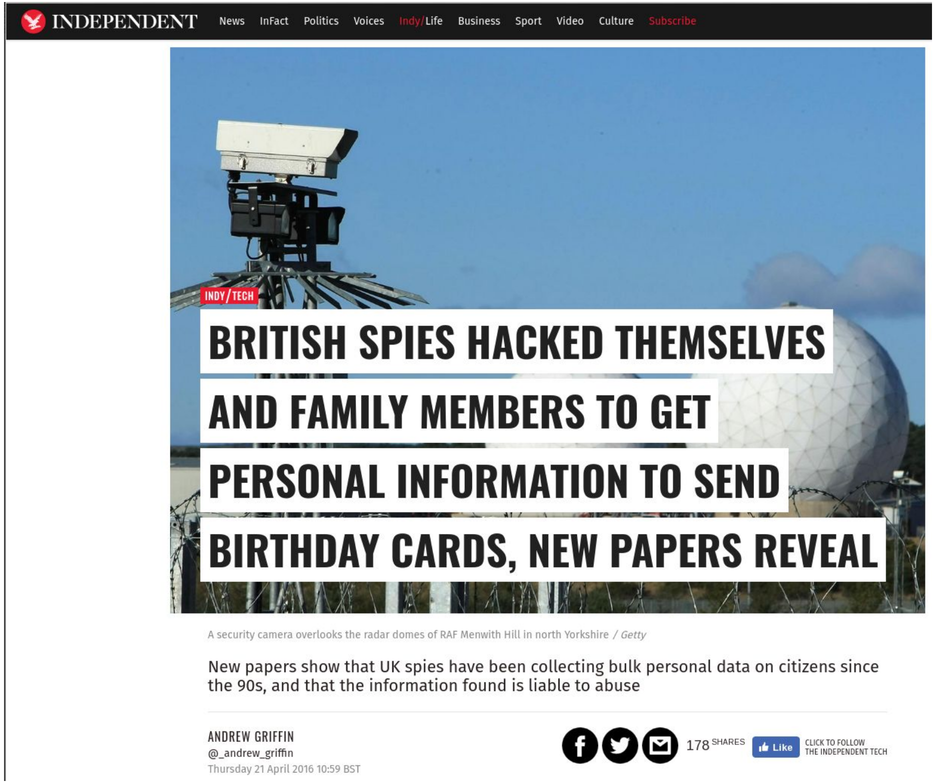
September 8th 2017

"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?



INDEPENDENT News InFact Politics Voices Indy/Life Business Sport Video Culture Subscribe

INDY/TECH

BRITISH SPIES HACKED THEMSELVES AND FAMILY MEMBERS TO GET PERSONAL INFORMATION TO SEND BIRTHDAY CARDS, NEW PAPERS REVEAL

A security camera overlooks the radar domes of RAF Menwith Hill in north Yorkshire / *Getty*

New papers show that UK spies have been collecting bulk personal data on citizens since the 90s, and that the information found is liable to abuse

ANDREW GRIFFIN
@_andrew_griffin
Thursday 21 April 2016 10:59 BST

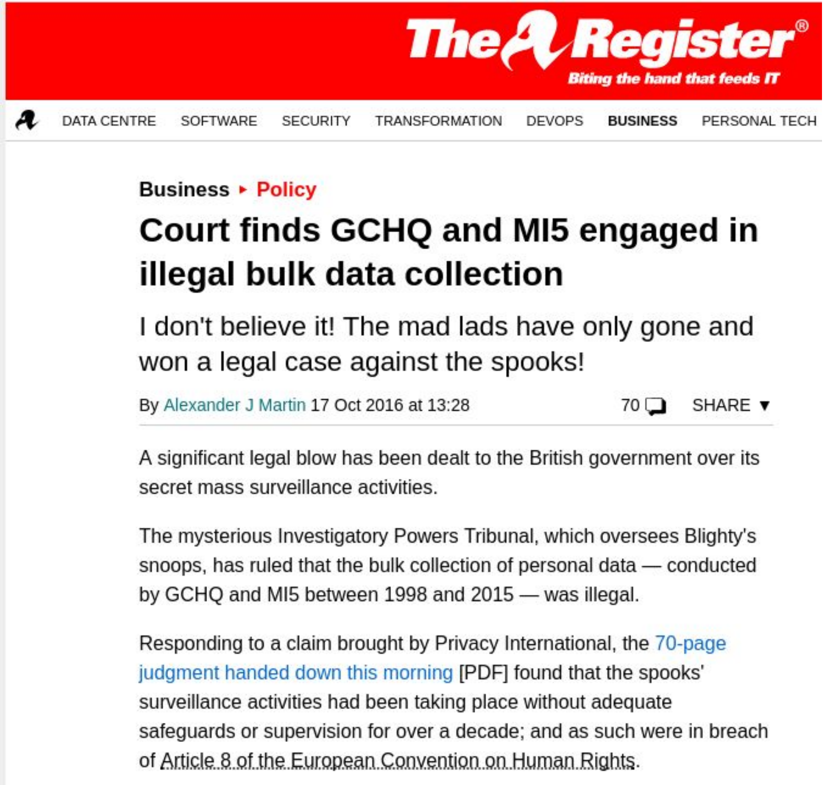
178 SHARES Like CLICK TO FOLLOW THE INDEPENDENT TECH

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?



Business ▸ Policy

Court finds GCHQ and MI5 engaged in illegal bulk data collection

I don't believe it! The mad lads have only gone and won a legal case against the spooks!

By Alexander J Martin 17 Oct 2016 at 13:28

A significant legal blow has been dealt to the British government over its secret mass surveillance activities.

The mysterious Investigatory Powers Tribunal, which oversees Blighty's snoops, has ruled that the bulk collection of personal data — conducted by GCHQ and MI5 between 1998 and 2015 — was illegal.

Responding to a claim brought by Privacy International, the 70-page judgment handed down this morning [PDF] found that the spooks' surveillance activities had been taking place without adequate safeguards or supervision for over a decade; and as such were in breach of Article 8 of the European Convention on Human Rights.

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

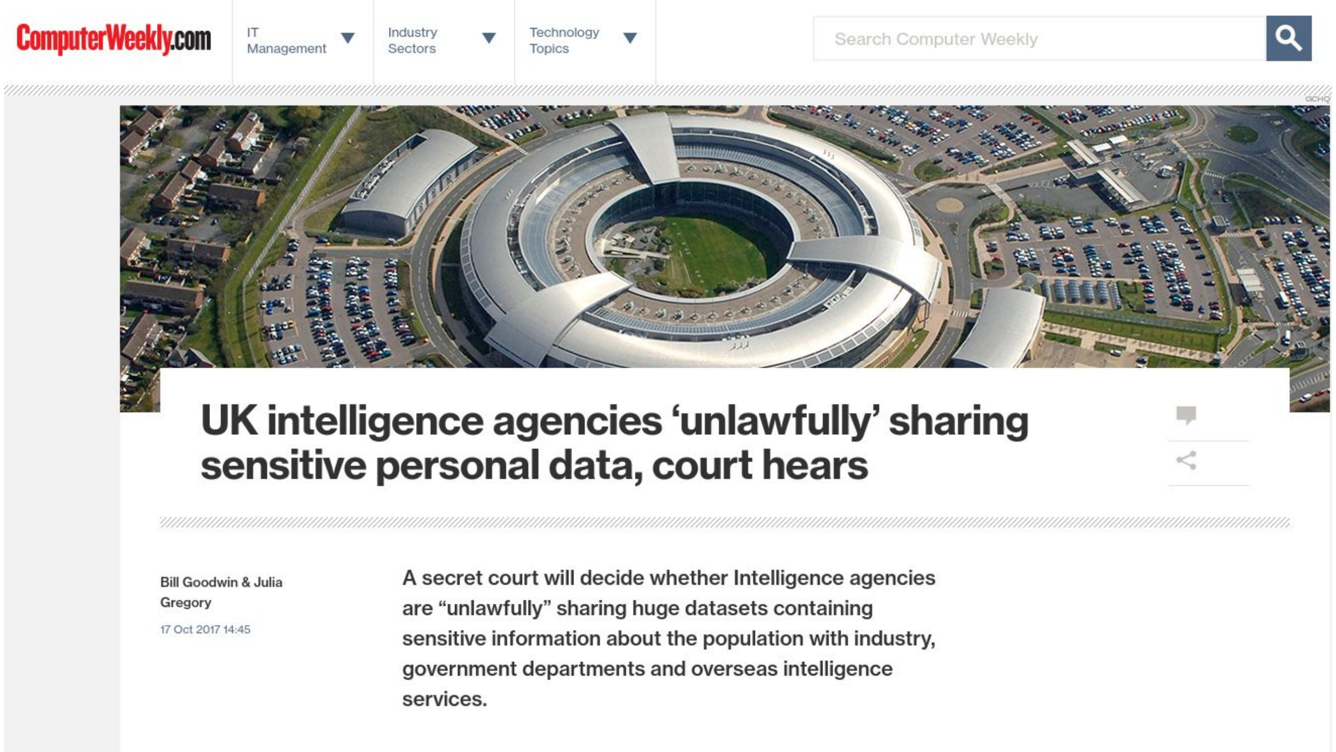
Published 21 September 2017

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?



UK intelligence agencies 'unlawfully' sharing sensitive personal data, court hears

Bill Goodwin & Julia Gregory

17 Oct 2017 14:45

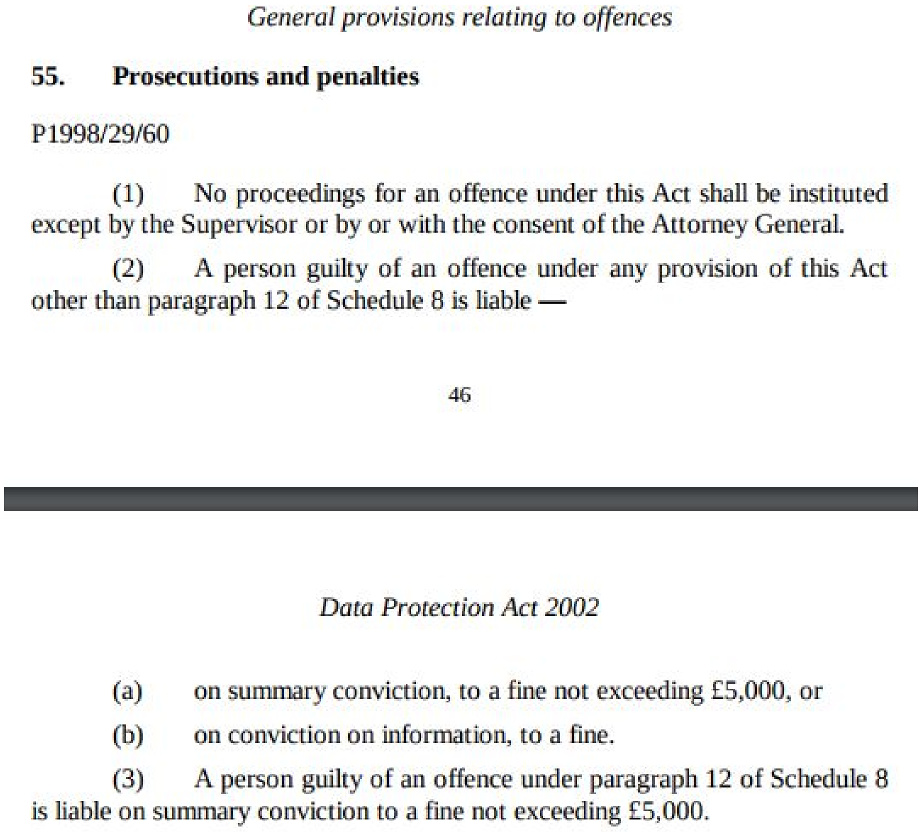
A secret court will decide whether Intelligence agencies are "unlawfully" sharing huge datasets containing sensitive information about the population with industry, government departments and overseas intelligence services.

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 —

46

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.

UK DPA 1998 - £500,000 fine

IoM DPA 2002 - £5,000 fine

Almost Zero disincentive to IoMG

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.