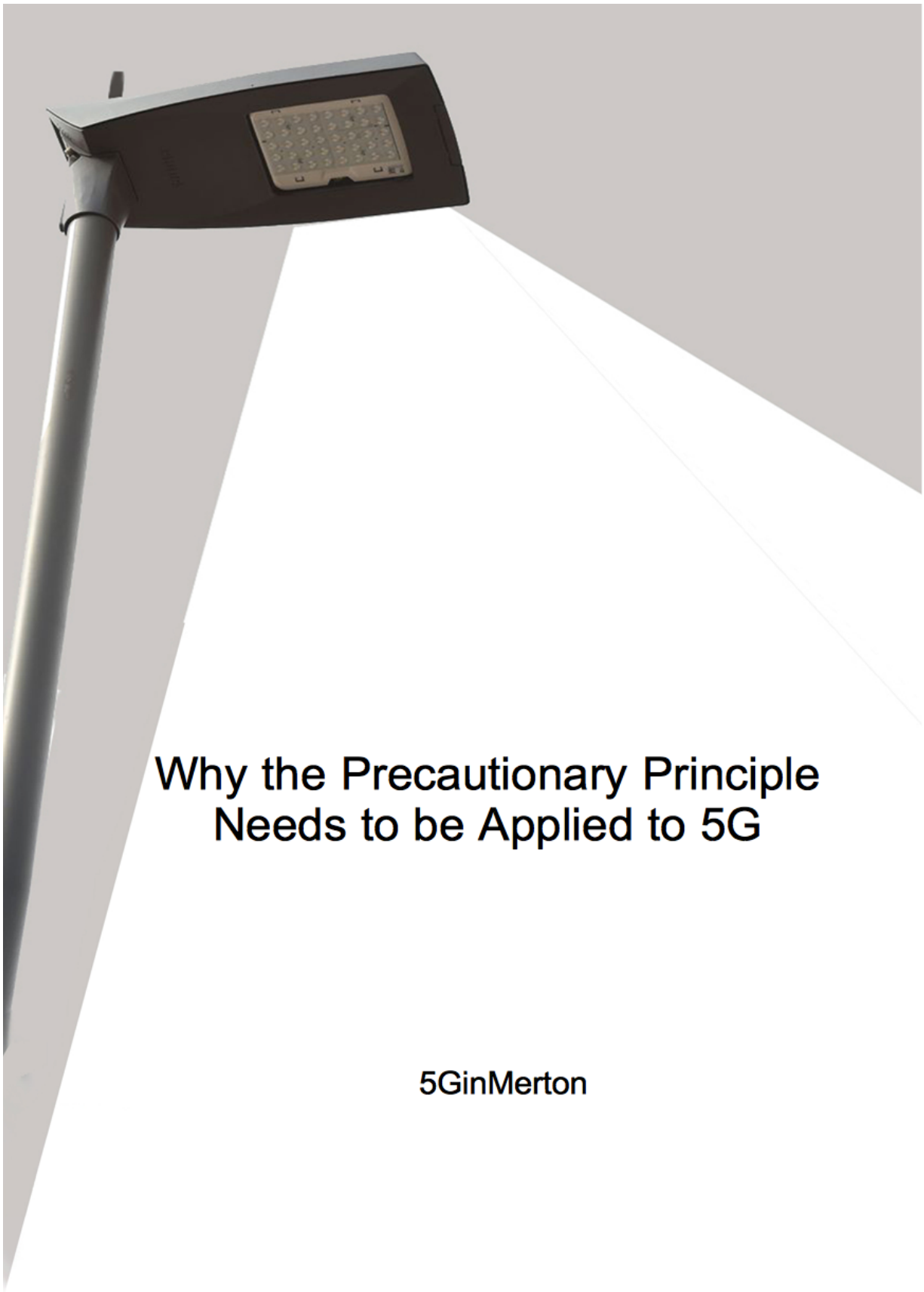


Why the Precautionary Principle Needs to be Applied to 5G

5GinMerton

Table of Contents

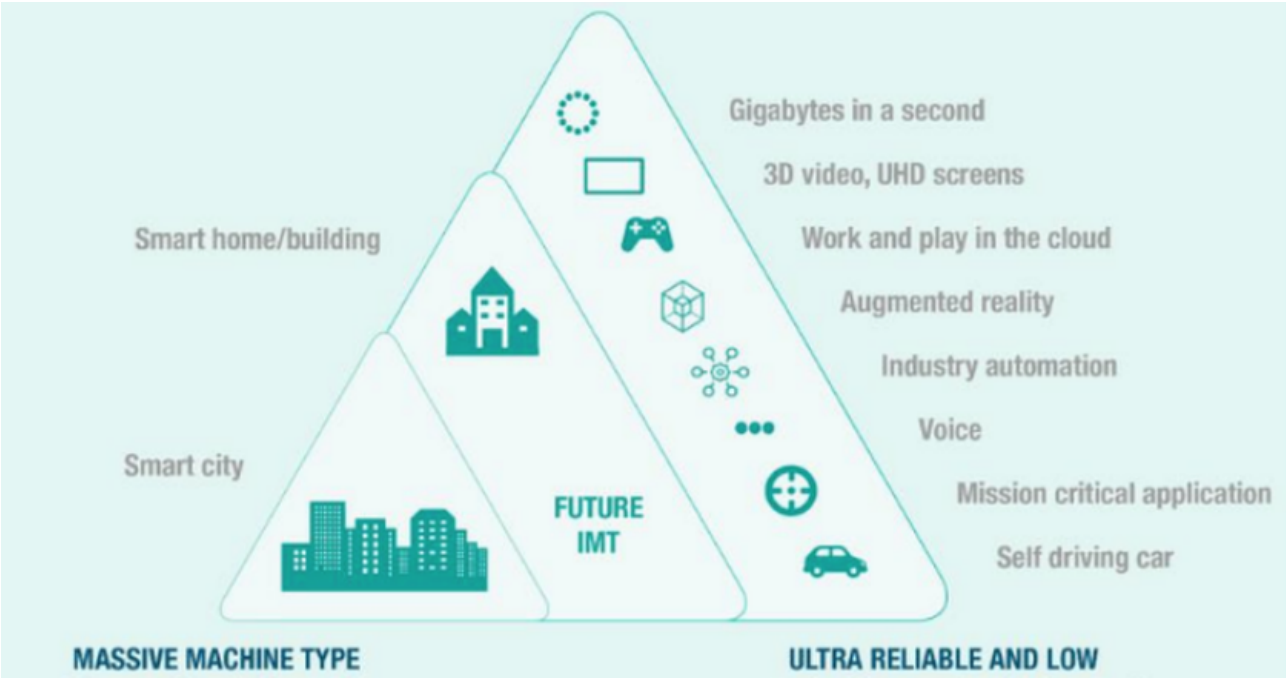
5G and how it will be more pervasive than other generations of network

5G encompasses previous generations 3G, 4G, 4G LTE as well as the 5G layer.
The internet of things (IoT) will be connected to the 5G layer and will be in homes, workplaces, smart motorways, smart railways, smart cities, autonomous cars. It's all in the governments own vision for 5G. It presents a huge challenge to our right to our privacy. To service such massive AI-enabled, machine to machine, communications, transmitters will be placed on streetlights every 3-5 houses length, close to homes, schools, hospitals, civic buildings and work places.

Large transmitters (75-85m in height) will now be under permitted development, so will no longer need to consult local communties. 5G is positioned as part of goverment's industrial strategy and it has decided to push it through in partnership with private companies using "barrier-busting taskforces".

Representations made at local authority level do not count. Dr David Drew MP points out "The electronic communications code has granted virtually unlimited powers to companies to construct, maintain or develop the current infrastructure without any planning permission. It is all done under delegated responsibility, which means that the general public do not even know what is going on, because normally these things are not publicised. There is little recourse unless the public take court action to stop it, but the means of doing so are limited. Even a private landowner has little authority to stop it. The matter needs to be looked into and properly investigated." The same forcing through of 5G infrastructiure is happening in North America as well. These documents show government's direction of travel.

- Next Generation Mobile Technologies: A 5G strategy for the UK- 8 March 2017
- DCMS Policy paper and Next Generation Mobile Technologies: An update to the 5G strategy for the UK- 19 Dec 2017- DCMS Policy paper)



Source: DCMS- Next Generation Mobile Technologies: An update to the 5G strategy for the UK

5G and Phased Array- Why it is important.

What it is

When researching 5G, many concerns bring up its use of millimeter wave frequency and its effects on biology. It seems, initially at least, many of the applications of 5G will not use this frequency. However, the other aspect about 5G which receives less attention but is critical to be aware of is the use of **phased array** in 5G. This video explains what phased array is simply and clearly: https://youtu.be/vtPPAnvJS6c

It's useful to understand the term **"collimation"** which is the is the ***focusing of a beam***. A laser pointer collimates light in a particular direction. Transmitters in an **array** (***array = a regular pattern e.g. 2 parallel lines such as streetlights***) which are then **phased** (***emit EMR in a time sequence***) lead to interference patterns with the effect of producing **focused beams**/collimation of EMR that can be **directed very rapidly**. Focussing of a beam increases the power of the signal.

Mark Steele, a weapons engineer contends that elaborate chipsets incorporating high-powered capacitors were being installed in Gateshead streetlights. A capacitor is like a battery where power is stored, but unlike a battery the power is released very rapidly, think of the old camera flash bulbs which charge up and then release its energy in a flash of light. So the increased power of the signal which comes from it being focussed like a laser pointer is further boosted from the capacitor.

He also identifies uploading/backhaul capability in the chipsets which brings in the issue of privacy

What is the significance of this?

The streetlights when grouped together form a parallel line arrangement/array, signals can be time-sequenced/phased to form a phased array. Among other things this is required for automated cars, part of the government's vision for 5G. Other points of note are:

- The focussing of the beam will allow the signals to push through buildings, other barriers and connect with smart devices
- These high powered beams and the devices they link to will pulse rapidly, affecting living things at a cellular level
- The technology could scan inside homes and build a picture inside. This person built a phased array in his garage: https://hackaday.com/2015/04/07/build-a-phased-array-radar-in-your-garage-that-sees-through-walls/
- If large capacitors are included in 5G-enabled public hardware, individuals can be rapidly targetted with high powered millimetre waves as used by the military for crowd-control (active denial weapons).

UK Safety Standards flawed and out of date

Pulsed, Directed and mm wave EMFs Omitted

Pulsed EMFs in most cases are much more biologically active than non-pulsed EMFs of the same average intensity. However, pulsations are ignored in the safety guidelines despite the fact that almost all of our current exposures are highly pulsed. 5G will be much more highly pulsed, not least to cater for the "handshaking" with the internet of things devices. The same is the case with concentrated directed beam radiation that comes with use of phased array transmission, specific to 5G. Studies on the effects of mm wave frequencies have been restricted to the military and are classified, how many of them relate to health is unclear. U.S Senator Blumenthal is unequivocal "I know of no reliable studies classified or otherwise that have been done about 5G"

Average EMF Intensity and Time Period as Basis for Predicting Safety is a Flaw

The assumption that average EMF intensities and average specific absorption rates (SAR) can be used to predict biological effects and therefore safety has time and again been shown to be false.

Many studies have shown that there are what have been called intensity windows where **a short intensity range of exposures to a particular EMF,** produce maximum effects but **lower or higher intensities, produce much lower effects**. Averaging can only be predictive of biological effects when one has linear dose-response curves. However the window effects studies clearly show that **dose-response curves are neither linear nor monotone**. They do not always increase with increasing exposure nor do they decrease with decreasing exposure. This clearly shows that exposures averages over 6 minutes or 30 minutes cannot predict biological effects and therefore safety. Averaging over any time period cannot be used in genuine safety guidelines. This flow due to taking a physics based approach to safety whilst ignoring the biological perspective.

Assumption that Health Effects can be Predicted Simply Based on Physics is False.

Biological heterogeneity (not of different people but of different responses of different cell types) is important. **This is not considered**. A research group using identical methodologies found different cell types repeatedly responded differently to the same EMF exposures.

Specific Absorption Rates (SAR) only looks at Thermal Effects and Ignores non Thermal Effects (non-ionising radiation).

In 2018 the U.S. gold standard National Toxicology testing Program (NTP) confirmed after extensive peer review that wireless radiation from mobile phones has real carcenogenic effect in at least 2 sites- heart schwannomas and brain tumours.

Senator Blumenthal previously mentioned was not the only one who knows of no reliable information on 5G and its effects on people, the telecoms industry don't either, prompting his comment "we're flying blind"

Safeguards are now out of date:

Our current standards were informed by ICNIRP and WHO which set levels in 1996. At that time the widely-held assumption was that radio frequency radiation used for (mobile phones, Wi-Fi, Bluetooth, surveillance tech etc) does not have sufficient energy to break chemical bonds therefore damaging DNA and mpacting on our health. This has now repeatedly been proven wrong experimentally.

A local resident suffering severely from the effects and of EMR and treated as a result in St George's Hospital sent a detailed FOI request to the Department of Health and PHE about health issues arising from non-ionising radiation. DoH and PHE point to this AGNIR report in response and quoted the following from it: ***"although a substantial amount of research has been conducted in this area, there is no convincing evidence that radio wave exposures below guideline levels cause health effects in either adults or children."***

The first thing I note is how out of date the report is (published in April 2012), the last study they cite is from 2011. They do mention the NTP study, the largest study of its kind to date, but just to say it is on-going. With its results published in 2018, it contrary to the PHE, amongst many other subsequent studies show that non-ionising/non-thermal radiation has significant health effects. The tkey findings were mobile phone radiation caused cancers in the heart and the brain, DNA damage in brain cells, heart muscle disease ad reduced birth weights. Tumours were sited mostly in the heart, brain and adrenal gland. A separate study started later in Italy by The Ramazzini Institute (RI) also found results consistent with the NTP study. The 2012 assessment of the UK Health Protection Agency, now PHE, is on shaky ground.

Interestingly, the DoH wrote they are aware of many people with the same symptoms as the local resident, but say these symptoms are not related to EMR below the safety guidelines. They also state in their FOI reply ***"Public Health England keeps emerging scientific studies worldwide under review and supports the scientific processes and officially mandated organisations described above. It is also aware of other reports and groups that have made pronouncements on this topic but gives greater weight to documents that use rigorous review processes and base their advice on the entire range of scientific information available."*** This does not appear to be the case when it comes to non-ionising radiation.

On the 25th of June 2019, The House of Commons debate on health effects of 5G and wireless radiation made clear MPs have found that their constituents are all being referred to the same out of date document by PHE/DoH and the cases of electrosensitivity are rising. Tonia Antoniazzi MP: "Following the publication of a paper on the AGNIR 2012 report in Reviews on Environment Health, the AGNIR was quietly disbanded. However, the inaccurate report is still on its website and is used to justify its advice to MPs and the public. When will the 2012 report be retracted because it is scientifcally inaccurate and out of date?"

"The Department for Education in England and the Department of Education in Northern Ireland have said that it is the responsibility of schools to carry out risk assessments before technologies are introduced and used. However, schools cannot safeguard pupils or staff through a risk assessment if they have been given inaccurate information. Can schools be accurately informed about the risks, so that they can fulfilll their responsibilities to safeguard children?"

Schools and parents could have been informed that wireless signals are a possible human carcinogen; that there is evidence of damage to fertility; and that there are adverse effects on brain development. Schools could have been advised to use wired technologies to prevent possible harm to children's health and development. The EU has sent a cautionary message about Wi-Fi in relation to school children, but only France has removed Wi-Fi from its primary schools.

Professor Anthony Miller, an advisor to WHO acknowledges that new science has emerged since 2011 when radio frequency radiation was classified as a 2b- a possible carncinogen like lead and DDT. Note, 2011 is the last year the studies included in PHE distributed AGNIR document go up to.

Miller says “if the International Agency for Research on Cancer (IARC) revealuated Radio frequency radiation it would be placed in Class 1- a human carcenogen and governments could not possibly ignore that”. An advisory committee to the IARC has recommended said radio frequency be reevaluated with high priority.

The Council for Europe Resolution 1815 does not agree with ICNIRP/PHE guidelines

The Council for Europe, a separate entity from the EU is a body which agrees minimum legal standards across Europe an beyond. It's up to states to decide whether they incorporate them. They do not accept the ICNIRP/PHE guidelines.

Here are 2 paragraphs from their resolution 1815 'The potential dangers of electromagnetic fields and their effect on the environment':

"5. As regards standards or threshold values for emissions of electromagnetic fields of all types and frequencies, the Assembly strongly recommends that the ALARA (as low as reasonably achievable) principle is applied, covering both the so-called thermal effects and the athermic or biological effects of electromagnetic emissions or radiation. Moreover, **the precautionary principle should be applied** when scientific evaluation does not allow the risk to be determined with sufficient certainty. Given the context of growing exposure of the population, in particular that of vulnerable groups such as young people and children, there could be extremely high human and economic costs if early warnings are neglected.

6.The Assembly regrets that, despite calls for the respect of the precautionary principle and despite all the recommendations, declarations and a number of statutory and legislative advances, there is still **a lack of reaction to known or emerging environmental and health risks and virtually systematic delays in adopting and implementing effective preventive measures. Waiting for high levels of scientific and clinical proof before taking action to prevent well-known risks can lead to very high health and economic costs, as was the case with asbestos, leaded petrol and tobacco."**

Trees, Plants and Animal Wildlife

Among other things the 5G signal is impeded by trees, particularly along the millimetre wave spectrum.

“Network Rail is aiming to cull 10 million trees, the stated aim however is to prevent branches and leaves from falling on the track.

The Guardian reported on the culling on 29/04/2018: “James Graham, from Manchester, said he saw thousands of trees being felled last week along a 10-mile section of the trans-Pennine route from Manchester to Leeds.

“I know they have to manage the trees, but this was excessive,” he said. “It looked like some kind of logging operation. I was sitting in the train and looking out at the countryside and all you could see was mile after mile of tree stumps and sawdust. They had felled trees which were a long way from the track. It was extreme.”

In the 2017 Autumn Budget, the Government announced an investment of £35 million to install trackside fibre and 5G network infrastructure along the Trans Pennine route between Manchester, Leeds and York. In light of this fact, is it credible this vast cull is to simply prevent leaves and branches from falling on the track?”

https://ehtrust.org/science/bees-butterflies-wildlife-research-electromagnetic-fields-environment/

https://www.youtube.com/watch?time_continue=139&v=P-CvaoCxCDY

Small mammals and birds and insects will be heavily impacted because of their large surface to volume ratios. The same thing will be true of plants where even large trees have their leaves and reproductive organs highly exposed. One of the consequences that Professor Martin Pall predicts that we will have huge conflagrations because EMFs make plants vastly more flammable.

The Balance of Evidence on 5G Safety

The Lancet from Dec 2018 echoes all the above.

A 'weight of evidence' approach is used by scientific and regulatory bodies to reach an assessment of scientific findings on a given area. This has already been done by independent groups in the case of radiofrequency EMR.

The worlds largest categorised online database of **peer-reviewed studies** on anthropogenic EMR has been constructed by Oceania Radiofrequency Scientific Advisory Association **https://www.orsaa.org/.** ORSAA is an independent organisation not linked to government or industry**.** They **evaluated** these studies and then found

- **68%** of **2266** studies covering humans, animals, plants and populations have demonstrated significant biological or health effects

- **89%** of experimental studied studies looking at oxidative stress (makes cells more susceptable to DNA Damage) showed **significant** effects (216 of 242)

Mark Hertsgaard and Mark Dowie in their special investigation for the Nation 29th March 2018 (article attached) describe how funding friendly research has perhaps been the most important tactic by the wireless telecoms, because it conveys the impression that the scientific community truly is divided.

Thus, when studies have linked wireless radiation to cancer or genetic damage – as Wireless Technology Research project (WTR), did in 1999; as the WHO's Interphone study did in 2010; and as the US government's NTP did in 2018 – the industry can point out, accurately, that other studies disagree.

A closer look reveals the industry's sleight of hand. When Henry Lai, a professor of bioengineering at the University of Washington, **analysed 326** safety-related studies completed between 1990 and 2006, he discovered that

- 56% found biological effects from mobile phone radiation

But when Lai recategorised the studies according to their funding sources, a different picture emerged:

- 67% of the independently funded studies found a biological effect, while 28% of the industry-funded studies did. These are similar to the figures ORSAA arrived at.

Lai's findings were replicated by a 2007 analysis in Environmental Health Perspectives, which concluded that industry-funded studies were **two and a half times less likely** than independent studies to find health effects.

The scientific evidence that cell phones and wireless technologies in general can cause cancer and genetic damage is not definitive, but it is abundant and has been increasing over time. Contrary to the impression that most news coverage has given the public:

- 90% of the 200 existing studies included in the National Institutes of Health's PubMed database on the oxidative effects of wireless radiation show its tendency to cause cells to shed electrons, which can lead to cancer and other diseases.

Martin L. Pall, PhD, Professor Emeritus of Biochemistry and Basic Medical Sciences, Washington State University on 23rd May 2019 compiled ***'8* Repeatedly Documented Findings Each Show that EMF Safety Guidelines Do Not Predict Biological Effects'**

He writes: "We know that there is a massive literature, providing a high level of scientific certainty, for each of eight pathophysiological effects caused by non-thermal microwave frequency EMF exposures. This is shown in from 15 to 39 reviews on each specific effect" (details of each review can be found here)

1. Lowered fertility, including tissue remodeling changes in the testis, lowered sperm count and lowered motility and other measures of lowered sperm quality, lowered female fertility including ovarian remodeling, oocyte (follicle) loss, lowered estrogen, progesterone and testosterone levels (that is sex hormone levels), increased spontaneous abortion incidence, lowered libido (25 reviews).

2. Neurological/neuropsychiatric effects including sleep disturbance/insomnia; fatigue/tiredness; headache; depression/depressive symptoms; lack of concentration/attention/cognitive dysfunction; dizziness/vertigo; memory changes; restlessness/tension/anxiety/stress/agitation; irritability (29 reviews).

3. Effects on cellular DNA including single strand and double strand breaks in cellular DNA and on oxidized bases in cellular DNA; also evidence for chromosomal mutations produced by double strand DNA breaks. These produce all of the important type of mutations, as described at the DNA level that have roles in cancer causation and in human whole organism mutation (24 reviews).

4. Apoptosis/cell death (an important process in production of neurodegenerative diseases that is also important in producing infertility responses) (15 reviews).

5. Oxidative stress/free radical damage (important mechanisms involved in almost all chronic diseases; direct cause of cellular DNA damage) (25 reviews).

6. Endocrine, that is hormonal effects; Includes changes in non-steroid and also steroid hormones (15 reviews).

7. Increased intracellular calcium levels, thought to be the cause in all other effects (16 different reviews).

8. Cancer including initiation, promotion and progression, further including tumor progression, tissue invasion and metastasis) (39 reviews)

The Government View

The Parliamentary Under-Secretary of State for Health and Social Care, Seema Kennedy MP put the government's position in the House of Commons debate on 5G and health. "A report containing an evidence review and recommendations was prepared for Government by the independent expert

group on mobile phones, under the chairmanship of Sir William Stewart. A major research programme was undertaken and the international exposure guidelines were adopted, with a commitment from industry that they would be followed." In the next section it is shown that Sir William's recommendations were in fact ignored and the adopted guidelines were from ICNIRP. It is unclear what the major research progrmme she mentions was and who carried it out.

Kennedy, defended PHE in regards to the information it uses to base its advice on. They seem to be using the weight of evidence approach, but it did appear from her statements the information used dates up to 2012.

"Expert groups in the UK and around the world have examined the evidence and published many comprehensive reports. In the UK, the advisory group on non-ionising radiation produced reports in 2003 and 2012. The Government have played their role in the international effort to learn more about the health effects of radio- wave exposure. They supported the dedicated mobile telecommunications and health research programme that ran from 2001 to 2012 and they continue to fund research."

"A challenge in understanding the evidence is that some studies report effects, while others do not. Sophisticated analyses are needed to draw studies together, considering their strengths and weaknesses and working out what they mean collectively, which is the role of expert groups. Simply counting or listing studies that have found effects is not an adequate way of assessing where the overall evidence lies."

`The experts groups work for the European Commission and the WHO but have not found any "clear evidence of adverse health effects if the ICNIRP guidelines are followed." It would be interesting to know, may be using an FOI the following:

- how many studies were analysed,
- the period they covered,
- if the funders of the studies where taken into account,
- how "clear evidence" is being defined in this case

The Balance of Evidence and The Precautionary Principle

The "precautionary principle" holds that society doesn't need absolute proof of hazard to place limits on a given technology.

If the evidence is sufficiently solid and the risks sufficiently great, the precautionary principle calls for delaying the deployment of that technology until further research clarifies its impacts.

The scientists' petition urges government regulators to apply the precautionary principle to 5G technology. Current safety guidelines "protect industry—not health," contends the petition, which "recommend[s] a moratorium on the roll-out of [5G]…until potential hazards for human health and the environment have been fully investigated by scientists independent from industry."

No scientist can say with certainty how many wireless-technology users are likely to contract cancer, but that is precisely the point: We simply don't know. Nevertheless, we are proceeding as if we do know the risk, and that the risk is vanishingly small. Meanwhile, more and more people around the world, including countless children and adolescents, are getting addicted to cell phones every day, and the shift to radiation-heavy 5G technology.

Conflict of Interests

For years, respectable American and European scientists carried out research supported by the Tobacco Industry Research Council, at a time when there was little government sponsorship of science. Only when bodies of evidence accumulated, making the dangers of tobacco undeniable, were tobacco-funded studies brought to an end. The achievements of the tobacco industry in manipulating science led Judge Gladys Kessler to confirm a verdict of racketeering that included manipulating institutions such as the American Medical Association and National Cancer Institute — both of which at various times worked to build a safe cigarette.

As GQ reported a decade ago, the telecommunications industry uses the same PR strategies, some of the same industry consultants and scientists to promote disinformation in defence of their addictive products. Further, in 2015 a Harvard expose tracked the revolving door between the FCC and the telecom industry and concluded that the FCC is a captured agency and that "Consumer safety, health, and privacy, along with consumer wallets, have all been overlooked, sacrificed, or raided due to unchecked industry influence."

Microwave News is an independent publication which has been going for 35 years and is an , trawling through its archive you can see theme of compromised studies and poor reporting of findings across many years. On 30 July 2007 it reported that the founder of ICNIRP and the former director of WHO's EMF project, Mark Repacholi revealed that up to half of WHO's EMF project funding came from wireless and electric utility industry groups

In 2007 Panorama broadcast 'WiFi Warning Signal' talks about the precautionary principle being ignored when it comes to WiFi, particularly in schools (children are far more biologically affected by it). The scientists featured say the standards of non-ionising radiation are based on a distored picture of the science which assumes the absence of thermal effects is the absence of harm. One of them is Professor Henry Lai mentioned in the previous section and is described as being "respected by both sides of the argument".

Former Chief Scientific Advisor to Margaret Thatcher and the Chairman of the Health Protection Agency (HPA) in 2007, Sir William Stewart was also featured in the programme. He looked at studies of the biological effects of mobile phones and WiFi for over a year and recommended the precautionary principle. The programme notes that the government favours the advice of Mark Repacholi of ICNIRP and WHO over its own advisor Sir William Stewart. Repacholi talks about the 'weight of evidence' approach, then Panorama reveals he used to work for the phone industry before and after joining the WHO as an expert witness, "defending their right right to site masts in controversial locations" He even casually says he is funded by industry!

The current director is of the WHO EMF project is Emilie van Deventer an electrical engineer who carried out industry-funded research to make signals pass through cell phone circuitboards faster and better. Would it not make more sense to have a medical doctor or biophysicist as the director when the primary aim is to ensure that health is not harmed by EMF?

For a fuller and more detailed picture of how the wireless telecoms industry money has influenced institutions, scientists, studies, regulators, communication of those studies to the public. Please see attached or click on the links:

- 'The ICNIRP Cartel and the 5G Mass Experiment' and
- 'How Big Wireless Made Us Think That Cell Phones Are Safe: A Special Investigation -The disinformation campaign and massive radiation increase behind the 5G rollout.' (a podcast with the jounalist discussing his investigation is on the page.

Insurers excluding cover for long-term non-ionising radiation exposure

During their aforementioned investigation Hertsgaard and Dowie could not find an insurance company willing to sell a product-liability policy covering mobile phone radiation. Unsurprising considering Lloyds of London and Swiss Re's position on the matter:

Lloyds of London

A recent commercial liability insurance renewal policy issued through a Lloyd's of London underwriter contained a liability exclusion clause about electromagnetic fields.

The clause excludes any compensation for claims:
"directly or indirectly arising out of, resulting from or contributed to by electromagnetic fields, electro-magnetic radiation, electromagnetism, radio waves or noise."

It is important that "radio waves" are explicitly included as they, specifically the microwave zone, are what enable wireless communications devices like cell phones, wi-fi, cordless phones etc.

After an inquiry seeking clarification about the exclusion language, CFC Underwriting LTD in London, the UK agent for Lloyd's, sent the following:

"The Electromagnetic Fields Exclusion (Exclusion 32) is a General Insurance Exclusion and is applied across the market as standard. The purpose of the exclusion is to exclude cover for illnesses caused by continuous long-term non-ionising radiation exposure i.e. through mobile phone usage."

Swiss Re (Insurers of insurance companies)

Direct quote from Swiss Re: "To allow for a functional network coverage and increased capacity overall, more antennas will be needed, including acceptance of higher levels of electromagnetic radiation. In some jurisdictions, the rise of threshold values will require legal adaptation. Existing concerns regarding potential negative health effects from electromagnetic fields (EMF) are only likely to increase. An uptick in liability claims could be a potential long-term consequence.

Other concerns are focused on cyber exposures, which increase with the wider scope of 5G wireless attack surfaces. Traditionally IoT devices have poor security features. Moreover, hackers can also exploit 5G speed and volume, meaning that more data can be stolen much quicker. A large-scale breakthrough of autonomous cars and other IoT applications will mean that security features need to be enhanced at the same pace. Without, interruption and subversion of the 5G platform could trigger catastrophic, cumulative damage. With a change to more automation facilitated by new technology like 5G, we might see a further shift from motor to more general and product liability insurance.

There are also worries about privacy issues (leading to increased litigation risks), security breaches and espionage. The focus is not only on hacking by third parties, but also potential breaches from built-in hard- or software "backdoors." In addition, the market for 5G infrastructure is currently focussed on a couple of firms, and that raises the spectre of concentration risk."

Privacy

5G will work with the internet of things, bulk data collection will result. Over and above the data collection from our phones and computers, data will be collected from smart meters, smart fridges, smart thermostats, smart vacuum cleaners, autonomous cars etc. With the government's desire for smart cities our movements within our towns will be collected in the future as well. With this data you can easily ascertain when someone is at home or not, household routines, their purchases. The 5G infrastructure envisioned by DCMS is ideal for continual surveillance and tracking of activities. We are in the age big data and there is massive growth of the data science industry as can be seen in the jobs market. This, in conjunction with the "fourth industrial revolution" of AI generating algorhithms to analyse and identify relationships between many sources data in an ever more refined way can easily make privacy a thing of the past. How can we then be a democratic society? Part of 5G's specification is its ability to rapidly focus and direct its signal (using phased array), it could scan inside homes, build a picture and track people's movements inside.
https://hackaday.com/2015/04/07/build-a-phased-array-radar-in-your-garage-that-sees-through-walls/

5G, like all radio wireless technology is relatively insecure and can be hacked. It does not take much imagination to understand that if functions of autonomous cars were to be hacked, the effects would be disasterous.

The IoT of things which are growing are used for spying already as James Clapper, director of national intelligence said in 2016 "In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials," Clapper told a Senate panel as part of his annual "assessment of threats" against the US.

In 2012, Former CIA director David Petraeus when speaking about IoT said "'Transformational' is an overused word, but I do believe it properly applies to these technologies," Petraeus enthused, "particularly to their effect on clandestine tradecraft."

Since then in addition to the IoT there is now the internet of living things, raising another dimension of ethical questions. This raises many possibilities of use where privacy is further deleted.

It's not only China, UK's Recent History on Respecting Privacy isTerrible

In December 2016 it was found that the government was breaking the law by indiscriminately collecting the nation's internet activity and phone records and letting hundreds of public bodies grant themselves access to these personal details with no suspicion of serious crime and no independent sign-off – meaning significant parts of its Data Retention and Investigatory Powers Act (DRIPA) were effectively unlawful.

DRIPA expired on 31 December 2016 – but the Government then replicated and vastly expanded the same powers in its new flagship surveillance law, the Investigatory Powers Act, which passed in November 2016

DRIPA forces communications companies to store every person's "communications data" – the who, what, when, where and how of every email, text, phone call, and internet communication, including those of lawyers, doctors, MPs and journalists.

This data is subject to an extremely lax access regime, which lets hundreds of organisations and government agencies – from police forces to HMRC – grant themselves access for a wide range of reasons that have nothing to do with investigating serious crime.

CJEU judges have ruled this regime breaches British people's rights because it:

- allows general and indiscriminate retention of all communications data
- does not restrict access to this data to the purpose of preventing and detecting precisely defined serious crime.
- lets police and public bodies authorise their own access, instead of subjecting access requests to prior authorisation by a court or independent body.
- does not provide for notification after the event to people whose data has been accessed.
- does not require that the data be kept within the European Union.

Since this legal challenge was launched on DRIPA, the Investigatory Powers Act ***has not only re-legislated for the powers found unlawful previously, but gone much further.***

The Act has dramatically expanded powers to gather data on the entire population, while maintaining the controversial lack of safeguards that resulted in legal challenge.

Under it, the state now also has access to every person's internet use – every website visited or app used – which service providers must generate and store for 12 months.

This creates vast databases of deeply sensitive and revealing personal information which – at a time when companies and governments are under increasingly frequent attack from hackers – creates a goldmine for criminals and foreign spies.

This data can be accessed by dozens of public authorities with no need for suspicion of criminality or prior sign-off from a judge or other independent official. These include the NHS, Department for Work and Pensions and Gambling Commission.

The Investigatory Powers Act has also legalised other unprecedented bulk spying powers – including bulk hacking, interception of phone calls and emails on an industrial scale and collection of huge databases containing sensitive information on millions of people – which could integrate records such as Oyster card logs and Facebook back-ups.

In June 2019, the High Court ruled part of the Investigatory Powers Act which gave Government powers to order private companies to store everybody's communications data, including internet history, so that state agencies can access it, was unlawful. The Court ruled this part of the Act is incompatible with people's fundamental rights because ministers can issue data retention orders without independent review and authorisation – and for reasons which have nothing to do with investigating serious crime

UK Government has repeatedly failed to Protect Data of it's citizens

The Royal Free NHS Foundation Trust and Google DeepMind AI

In 2017 it was found that The Royal Free NHS Foundation Trust in London "failed" to comply with data protection rules when it gave 1.6 million patient records to Google-owned artificial intelligence company DeepMind for a trial, the Information Commissioner's Office ruled as it ordered tighter guidelines.

Google had access to a trove of patient information, including medical records for the last five

years.

The Trust and Google did not properly inform patients how their details were going to be used in the test, which used technology to monitor and diagnose acute kidney injury, the commissioner said following a year-long investigation.

The trial, which began in 2015, used technology to track patients' symptoms and send alerts to doctors through an app called Streams in the event of a drastic change in their health. It was designed to look for acute kidney injury, which affects up to 18 per cent of those admitted to hospital.

As part of the deal between the Trust and Google, the internet giant gained access to sensitive patient information such as HIV status, mental health history and abortions. The Royal Free did not tell patients that Google's DeepMind would have access to such information, but said it had "implied consent" because patients knew the Streams app offered "direct care".

The ICO ruled the deal was illegal, but did not plan to fine the Royal Free.

MI5

In June 2019 MI5 was found to have been unlawfully retaining innocent people's data for years.

It also failed to give senior judges accurate information about repeated breaches of its duty to delete bulk surveillance data, and has been criticised for mishandling sensitive legally privileged material.

The IPA provides the security services with extremely broad powers, under warrants issued by 'Judicial Commissioners', to hack computers and phones and intercept people's communications. These powers allow the Government to carry out "bulk surveillance" on huge numbers of people who are of no intelligence interest. That information is then stored by the security services for potential investigations in the future.

The Investigatory Powers Commissioner's Office (IPCO) is responsible for ensuring that privacy protections contained in the IPA are upheld, including safeguards around storage and timely deletion of data are met.

Following the initial revelation MI5 had breached IPA privacy safeguards, a series of 10 documents and letters from MI5 and IPCO have revealed more detail of those breaches, including that MI5 has failed to meet its legal duties for as long as the IPA has been law.

Despite heavy redaction by MI5, the documents reveal how a litany of failures and false assurances has led to what the Investigatory Powers Commissioner, Lord Justice Fulford, has concluded is the **"undoubtedly unlawful"** conduct of the UK's leading security service.

The documents show:

- ILLEGAL ACTIONS: The Commissioner concluded that the way MI5 was holding and handling people's data was "undoubtedly unlawful", setting out that: "Without seeking to be emotive, I consider that MI5's use of warranted data... is currently, in effect, in 'special measures' and the historical lack of compliance... is of such gravity that IPCO will need to be satisfied to a greater degree than usual that it is 'fit for purpose'".
- MI5 KNEW FOR THREE YEARS BEFORE INFORMING IPCO: MI5 failed to maintain key safeguards, such as the timely destruction of material and the protection of legally privileged material. This, says Lord Justice Fulford created "serious compliance gaps" in its legal duties. Shockingly, these gaps first became clear to MI5 staff in January 2016, and the MI5 board in January 2018, but were only brought to IPCO's attention in February 2019. Even then Fulford accuses MI5 officials of continuing to use "misleading euphemism" when describing their failure.
- FALSE ASSURANCES: Warrants for bulk surveillance were issued by senior judges (known as Judicial Commissioners) on the understanding that MI5's data handling obligations under the IPA were being met - when they were not. The Commissioner has pointed out that warrants would not have been issued if breaches were known. The Commissioner states that "it is impossible to sensibly reconcile the explanation of the handling of arrangements the Judicial Commissioners were given in briefings…with what MI5 knew over a protracted period of time was happening."

A senior MI5 official acknowledges that personal data collected by MI5 is being stored in "ungoverned spaces", while the MI5 legal team claims there is "a high likelihood [of material] being discovered when it should have been deleted, in a disclosure exercise leading to substantial legal or oversight failure".

And in an example of the disrespect the Government has for transparency and the public's right to know, it has applied for further details on MI5's breaches to be provided to the Court through **secret evidence and private hearings**.

The IPA still allows the state to collect the content of people's digital communications and records about those communications created by our devices, and hack computers, phones and tablets on an industrial scale. It also allows the creation and linking of huge 'bulk personal datasets'. The state can keep data on these databases even if it does not suspect individuals of a crime or other threat. This is being challenged.

The UK government has built a surveillance regime more extreme than that of any other democratic nation, abandoning the very rights and freedoms terrorists want to attack.

Private corporations and government agencies are engaged in unwarranted bulk data collection, which can be rapidly stored and sifted. 5G, a relatively insecure technology, can scan within buildings and through clothing using phased array transmitters. When used in conjunction with facial recognition as the police have done in Wales (in the absense of a legal framework), AI, IoT, automomous cars and smart cities more data can be collected in ever finer detail enabling more complex relationships between data to be made, thus it does not take much to see the huge potential abuse of power this represents. With 5G, the infrastructure for the punitive social-credit system as

used in parts of China where individuals, groups or populations can be targetted would be in place in the UK. A democracy yes, but one in which laws and safeguards have been repeatedly broken and where data-gathering on its population has been the most intense and indiscriminate.

Tech Corporations violating our privacy

https://www.wired.com/2012/05/google-wifi-fcc-investigation/-An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle- Google Street cars breaching privacy of households as they pass by mapping the area

https://www.dailymail.co.uk/sciencetech/article-2950081/It-s-not-just-smart-TVs-home-gadgets-spy-internet-giants-collecting-personal-data-high-tech-devices.html TVs and other seemingly innocuous devices, voice recording and filming us and sending back the data.

https://www.bbc.co.uk/news/world-us-canada-37447016 State hackers stole half a billion Yahoo users' details. It took Yahoo 2 years to make knowledge of the breach public.

Alternatives to 5G

The UK is behind in 5G technology, China leads the world, but the UK has advantages when it comes to far more secure, safe and better performing technology of fibre and Li-Fi. Britain is in the lead when it comes to researching and building Lifi components which can now fit into phones. It is almost ready for the comsumer market. Indeed, I saw it being demonstrated at the Institute of Physics on a phone and on a tablet. It can work with safe LED lights which do not disrupt our circadian rhythm, they don't have the health issues which 5G or previous generations of mobile networks have. They are also more secure and private as the network you connected to only goes as far as the beam of light you are using. So there are lots of discrete contained networks. The bandwith avaialble on the light spectrum is 1000 times more than what is available on the radio. Harald Haas, who was the Institute of Physics explains the technology below, which has further advanced since he gave his presentations in 2011and 2015:
https://www.ted.com/talks/harald_haas_wireless_data_from_every_light_bulb
https://www.ted.com/talks/harald_haas_a_breakthrough_new_kind_of_wireless_internet

Compared to most, we are in a better position to implement high speed fibre. Much of the infrastructure in terms of routing and provision of fibre is further advanced. Wired networks are safe, far more secure, for instance the Google mapping cars could not have taken data from WiFi home networks it passed. It is also faster and more reliable than wireless. So there are alternatives which would benefit the UK's economy, are better for our health and well-being, are far more secure.

The benefits to the economy of 5G is dubious but it is being pushed through as part of the governments industrial strategy. The vision for 5G , where it is makes every item smart whilst harnessing AI would mean a massive change for society and for quality of life, yet the implications have not been discussed among the wider public.

"…the business case for the investment required for the deployment of 5G is not yet established…. the Government and wider public sector can therefore play a vital role in driving early demand as a major purchaser of 5G services as well as helping to address issues around public perception…"
(p8/9, Next Generation Mobile Technologies: A 5G Strategy for the UK, March 2017)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/597421/07.03.17_5G_strategy_-_for_publication.pdf

What we want

Writing this document has helped answer these questions for me, hopefully it will for others too:

1. We've used 1-4G for years so what's the problem now?

- Latest most comprehensive studies show current exposures have significant health impact
- standards out of date (from 1996), based on false assumptions
- densification/pervasiveness- IoT, streetlight transmitters
- Lloyds of London and Swiss RE (insurer which insures insurance companies) will not insure telcos when it comes to wireless comms because it could potentially lead to the next long term health crisis like asbestos or tobacco.

2. 5G uses frequencies that have been used before e.g. 700 MHz, this was used by digital television (Freeview) until this was changed, why the alarm now?

- When implemented in 5G there will be a massive increase in pulsed EMF,
- 5G uses focussed beam EMR
- Based on phased array tech

3. The evidence is that it's safe. It wouldn't be rolled out otherwise?

- No independent studies looking at the health effects have been done on for 5G
- Independent expert groups who have analysed thousands of studies into the health effects radio-frequency EMR have found the preponderance of evidence points to it causing cumulative harm.
- The evidence that "non-ionising radiation" is biologically active and has the energy to break chemical bonds causing oxidative stress and DNA damage is particularly clear. However, our out of date safety guidelines are based on **assumption** that this is not the case.
- Bodies that pronounce on safe exposure levels have serious funding conflicts of interests

4. If transmitters are nearer our homes they will be of lower power, won't they?

- Phased-array focussed beams increases power.
- Focused, mm wave frequency-specific to 5G, is weapons based crowd control technology
- It is highly unlikely the harm of electrosmog would be restricted to insects, small animals and plants but even if this was the case the knock on effect on humans would be huge.

5. Many have given away privacy for convenience, what difference will 5G make?

- It will be possible for 3rd parties with access to IoT data to know where you are and when, such as whether you are at home or not as well as your patterns of activity/consumption within the home.
- Even more bulk data collection in finer detail which is then mined using AI.
- Wireless by its very nature is far more susceptible to hackers than wired
- The 5G technology and the way it is being implemented means its surveillance potential can be likened to our communities being under a giant airport scanner
- It has the potential for singling out individuals and implementing a social-credit system
- UK government's track record on privacy is very bad and has not shown it can be trusted with such sensitive personal information.
- Public bodies work for us and are supposed to be transparent not private individuals.

This is why many people and myself want:

1. **Proven safe and non-intrusive (privacy) technology.**

2. **The precautionary principle to be applied to 5G.**