Is Your Phone Spying on You? Computer Scientists Reveal What's Hiding in Your Apps

People love their smartphones, but did you know they could be spying on you? A recent study by computer scientists from New York University and UC San Diego uncovered the hidden dangers of spyware apps. These apps are not only difficult to detect, but they can also leak your sensitive information without your knowledge. The team warns that it's important to be aware of this issue and take steps to protect yourself and your privacy.

"This is a real-life problem and we want to raise awareness for everyone, from victims to the research community," says Enze Alex Liu, the first author of the paper, in a **university release**.

Spyware apps are often marketed as tools to monitor children or employees, but they can also be used by abusers to secretly spy on their partners. These apps are designed to record everything that happens on a victim's device, including text messages, emails, photos, and even phone calls. The abusers can then access this information remotely through a web portal. The use of spyware apps has been on the rise, with a significant increase in their usage in recent years.

To find out if your device has been infected with a spyware app, you can check your privacy dashboard and the list of all apps in your device's settings. However, these apps are specifically designed to remain hidden, making them **difficult to detect**.

The study focused on analyzing 14 leading spyware apps for **Android phones.** While Google does not allow the sale of these apps on its official app store, they can still be downloaded separately from the web. This is in contrast to **iPhones**, which do not allow such "side-loading" of apps, making spyware apps less prevalent on this platform.

So, how do spyware apps work?

These apps run secretly on a device, collecting a wide range of sensitive information **such as location data**, text messages, calls, and even audio and video recordings. Some apps can even stream live audio and video. All this data is then sent to the abuser through an online spyware portal.

The researchers discovered that spyware apps use various techniques to collect data without the user's knowledge. For example, some apps utilize invisible browsers to stream live video from the device's camera to the spyware server. Other apps can record phone calls by **activating the device's microphone** or even the speaker function. Additionally, some apps take advantage of accessibility features designed for visually impaired users to record keystrokes and other sensitive information.

To make matters worse, these apps can hide themselves on the victim's device. They can avoid appearing in the app launcher or masquerade as harmless icons like **"Wi-Fi" or "Internet Service."** Some apps even accept commands through SMS messages, with a few of them executing these commands regardless of their source. In extreme cases, a command could be sent to remotely wipe the victim's phone.

Data security is another major concern. Many spyware apps transmit the collected data through unencrypted channels, making it vulnerable to interception. Some apps store this data in publicly accessible URLs, allowing anyone with the link to access it. Furthermore, some apps retain sensitive data even after the user has deleted their account or stopped using the app.

How can you protect yourself from spyware?

The researchers recommend that **Android devices** enforce stricter requirements for app icons to prevent them from hiding. They also suggest the implementation of a dashboard for monitoring apps that start automatically. Additionally, they propose adding a visible indicator to the user when the microphone or camera is being used by an app.

It's important to note that the researchers have shared their findings with the affected app vendors, but they have not received any responses yet. To prevent misuse, they have chosen to make their work available only to individuals who can demonstrate a legitimate need for it.

The fight against spyware requires a collective effort from various stakeholders, including individuals, smartphone manufacturers, app stores, and law enforcement agencies. As individuals, we must stay vigilant and take steps to protect our privacy. Here are some key measures you can take to safeguard your device from spyware:

Stick to Official App Stores: Avoid downloading apps from unknown sources or third-party websites. Stick to trusted app stores like Google Play Store or Apple App Store, as they have strict security measures in place to minimize the risk of spyware-infected apps.

Check App Permissions: Pay attention to the permissions requested by apps during installation. Be cautious if an app asks for unnecessary permissions that seem unrelated to its functionality. If an app requests access to your microphone, camera, or other sensitive data without a legitimate reason, it could be a red flag.

Regularly Update Your Device: Keep your smartphone's operating system and apps up to date. Developers release regular updates to address security vulnerabilities and enhance overall device security. By staying up to date, you ensure that your device has the latest security patches to fend off potential spyware threats.

Install Antivirus Software: Consider installing reputable antivirus or anti-malware software on your smartphone. These applications can scan your device for any malicious software, including spyware, and provide real-time protection against potential threats.

Be Mindful of App Reviews: Before installing an app, take a moment to read user reviews and ratings. Pay attention to any suspicious or negative reviews that mention privacy concerns or unusual behavior. This can help you make informed decisions about which apps to trust.

Regularly Review App Permissions: Periodically review the permissions granted to installed apps on your device. Revoke unnecessary permissions from apps that do not require access to certain data or functions. Limiting app permissions can minimize the risk of unauthorized access to your personal information.

Protect Your Device with Strong Passwords: Secure your device with a strong password, PIN, or biometric authentication. This adds an extra layer of protection, making it more difficult for unauthorized individuals to install spyware or gain access to your device.

Educate Yourself and Spread Awareness: Stay informed about the latest spyware threats and share this information with friends and family. By raising awareness about the dangers of spyware, we can collectively work towards creating a safer digital environment.

Remember, your privacy is valuable, and taking proactive steps to protect it is essential in today's digital age. By following these guidelines and staying informed, you can reduce the risk of falling victim to spyware and ensure your personal information remains secure.

Last week my daughter-in-law stopped by to take my wife out for her birthday dinner when I was sitting at the kitchen table. My wife was putting away groceries she had brought in from the car and was putting them away and much to my surprise I saw something that I have been aware of but never knew how simple it is to ping your cell phone.

My daughter-in-law's husband is an over the road long haul trucker. I knew where he was going earlier in the week but I asked the question about where he was now. My daughter-in-law popped out her **5G** "Smart" phone and the next thing I saw was a highway map on her phone screen. She tightened the image on screen and she told me was on a highway in North Carolina to make his second delivery. Reading and understanding how all this occurs is one thing but to seeing a live in motion target on the cell phone screen is something different. She continued by showing me where her children are at the exact moment. One was home sleeping after work, another was at her job at the local Cracker Barrel, another was working on his brakes of his car. They

have six children and she keeps tabs on them as needed. My daughter-in-law is a nurse and works 12-hour shifts and likes to keep track of them all.

My daughter-in-law virtually lives with her cell-phone, uses it to make small purchases through the "Near Field Communications" features at gas stations, convenience stores, hospital vending machines, cafeteria, alarm clock, getting take-out lunch, etc. Three years ago I tried to warn her about the **5G** wireless EMF/EMR radiation factor and the so-called vaccines being loaded with the Spike Protein. She is one of those who "know it all" and will not hear anything about the risks and negatives about **5G** cell phones. She is not interested in listening period. I am definitely not an uninformed person, in fact, I try to be on the cutting edge of technology.

It seems to me that people will believe what they want to believe and turn off their minds to the dangers of technology. I have been studying wireless energy and its many issues since the fall of 1996 when it was reported that bee keepers were losing their colonies to the dangers of EMF/EMR radiation poisoning. Many physicians were warning the public in 2020 about the connection with so-called vaccines and EMF/EMR. Dr. Sherri Tenpenny and Dr. Judy Mikovits said in the fall of 2020 that millions would die from the "gene" therapy being passed off as vaccines. At this point in time, estimates of those who have died range, from 25-million to 30-million, since the Covid-19 scam was introduced on the *"Diamond Princess"* cruise ship in January of 2020. It is not necessary to go into that story here but we know that **5G** is very much entwined as part of the problem.

You can't have **5G** without an important element that enables it to function as planned. Cesium-137 is a radioactive isotope and a basic factor to **5G**. The link to the Environmental Pollution Agency page can be found at the following link below:
Radionuclide Basics: Cesium-137 | US EPA
https://www.epa.gov/radiation/radionuclide-basics-cesium-137

The EPA site makes it very clear that Cesium-137 is a hazard to humans. The section on Cesium and Health is crystal clear about its potential harm.

Cesium and Health
External exposure to large amounts of Cs-137 can cause burns, acute radiation sickness and even death. Exposure to such a large amount could come from the mishandling of a strong industrial source of Cs-137, a nuclear detonation or a major nuclear accident. Large amounts of Cs-137 are not found in the environment under normal circumstances.

Exposure to Cs-137 can increase the risk for cancer because of the presence of high-energy gamma radiation. Internal exposure to Cs-137 through ingestion or inhalation allows the radioactive material to be distributed in the soft tissues, especially muscle tissue, which increases cancer risk.

The Cesium-137 isotope is essential for any and all **5G** devices to function as designed to function. It is what is used to maintain accuracy of atomic clocks, which set the standard for clock time around the world. Because it cycles at 60 beats to a minute it enables the world of wireless communications and data transfer between devices, people, businesses, etc. With a half-life of 30.7 years it is ideal for any electronic system of communications.

Older cell phones with locator chipsets were inadequate for police and EMS to find the precise locations of 9/11 calls. Previous cell phones were limited to a target location within about two-hundred feet. The "smart" phones being purchased today from Apple, Samsung, and others are equipped with the Cesium-137 isotope that will locate an emergency call to a location of two-meters or less than six feet. That is an important benefit if you live in a multi-story apartment building and have an emergency requiring you to make a 9/11 call.

Non-Ionizing and Ionizing Radiation

There are two kinds of radiation: non-ionizing radiation and ionizing radiation.

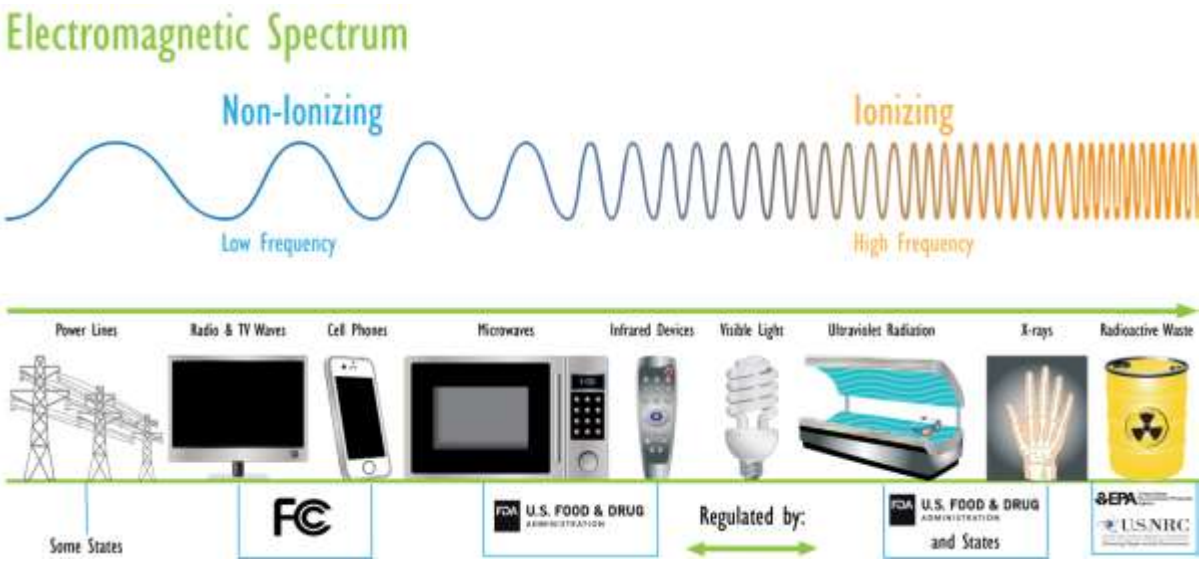
Non-ionizing radiation has enough energy to move atoms in a molecule around or cause them to vibrate, but not enough to remove electrons from atoms. Examples of this kind of radiation are radio waves, visible light and microwaves.

Ionizing radiation has so much energy it can knock electrons out of atoms, a process known as ionization. Ionizing radiation can affect the atoms in living things, so it poses a health risk by damaging tissue and DNA in genes. Ionizing radiation comes from x-ray machines, cosmic particles from outer space and radioactive elements. Radioactive elements emit ionizing radiation as their atoms undergo radioactive decay.

Radioactive decay is the emission of energy in the form of ionizing radiation. The ionizing radiation that is emitted can include alpha particles, beta particles and/or gamma rays. Radioactive decay occurs in unstable atoms called radionuclides.

Electromagnetic Spectrum

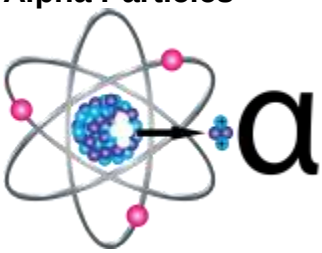
The energy of the radiation shown on the spectrum below increases from left to right as the frequency rises.



EPA's mission in radiation protection is to protect human health and the environment from the ionizing radiation that comes from human use of radioactive elements. Other agencies regulate the non-ionizing radiation that is emitted by electrical devices such as radio transmitters or cell phones (See: Radiation Resources Outside of EPA).

Types of Ionizing Radiation

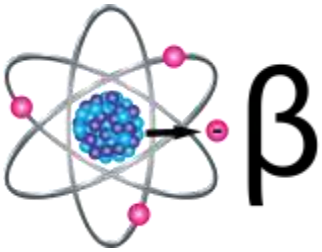
Alpha Particles



Alpha particles (α) are positively charged and made up of two protons and two neutrons from the atom's nucleus. Alpha particles come from the decay of the heaviest radioactive elements, such as uranium, radium and polonium. Even though alpha particles are very energetic, they are so heavy that they use up their energy over short distances and are unable to travel very far from the atom.

The health effect from exposure to alpha particles depends greatly on how a person is exposed. Alpha particles lack the energy to penetrate even the outer layer of skin, so exposure to the outside of the body is not a major concern. Inside the body, however, they can be very harmful. If alpha-emitters are inhaled, swallowed, or get into the body through a cut, the alpha particles can damage sensitive living tissue. The way these large, heavy particles cause damage makes them more dangerous than other types of radiation. The ionizations they cause are very close together - they can release all their energy in a few cells. This results in more severe damage to cells and DNA.

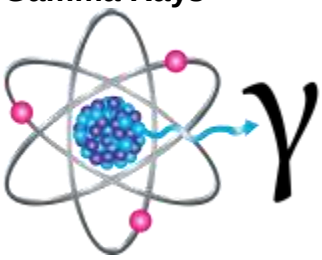
Beta Particles



Beta particles (β) are small, fast-moving particles with a negative electrical charge that are emitted from an atom's nucleus during radioactive decay. These particles are emitted by certain unstable atoms such as hydrogen-3 (tritium), carbon-14 and strontium-90.

Beta particles are more penetrating than alpha particles, but are less damaging to living tissue and DNA because the ionizations they produce are more widely spaced. They travel farther in air than alpha particles, but can be stopped by a layer of clothing or by a thin layer of a substance such as aluminum. Some beta particles are capable of penetrating the skin and causing damage such as skin burns. However, as with alpha-emitters, beta-emitters are most hazardous when they are inhaled or swallowed.

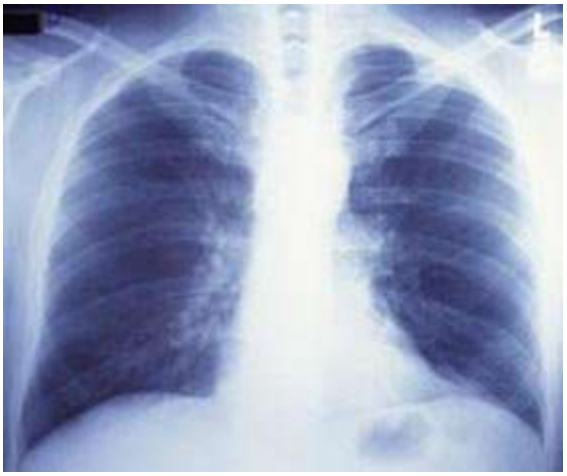
Gamma Rays



Gamma rays (γ) are weightless packets of energy called photons. Unlike alpha and beta particles, which have both energy and mass, gamma rays are pure energy. Gamma rays are similar to visible light, but have much higher energy. Gamma rays are often emitted along with alpha or beta particles during radioactive decay.

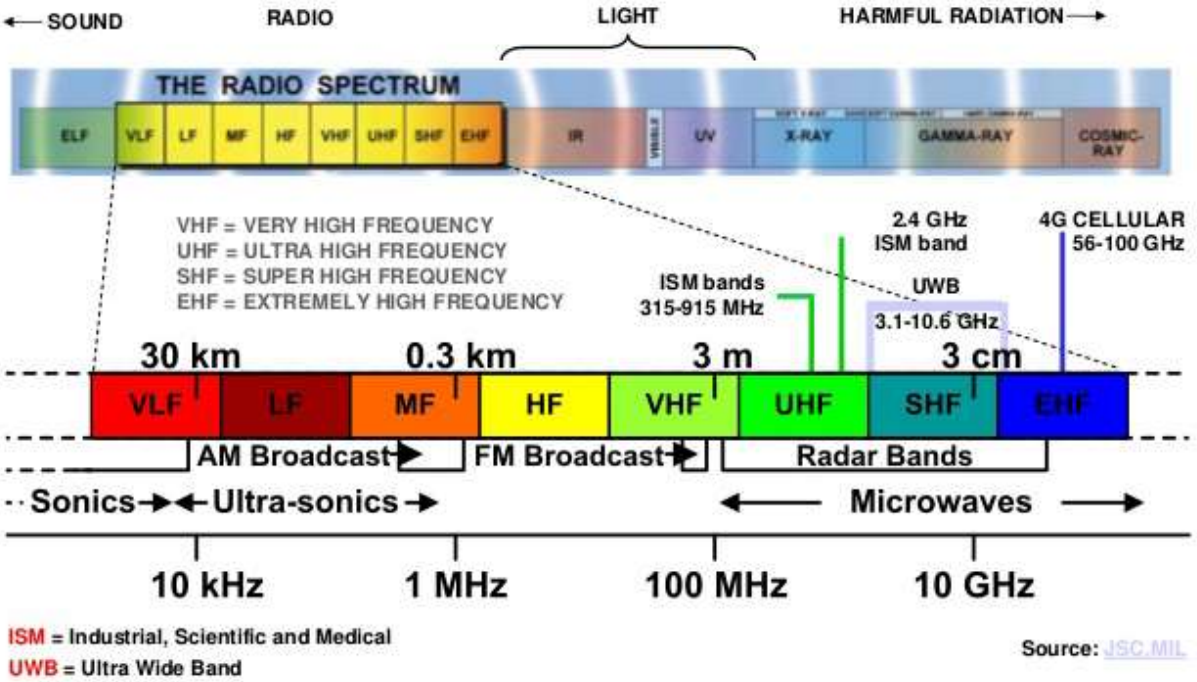
Gamma rays are a radiation hazard for the entire body. They can easily penetrate barriers that can stop alpha and beta particles, such as skin and clothing. Gamma rays have so much penetrating power that several inches of a dense material like lead, or even a few feet of concrete may be required to stop them. Gamma rays can pass completely through the human body; as they pass through, they can cause ionizations that damage tissue and DNA.

X-Rays



Because of their use in medicine, almost everyone has heard of X-rays. X-rays are similar to gamma rays in that they are photons of pure energy. X-rays and gamma rays have the same basic properties but come from different parts of the atom. X-rays are emitted from processes outside the nucleus, but gamma rays originate inside the nucleus. They also are generally lower in energy and, therefore less penetrating than gamma rays. X-rays can be produced naturally or by machines using electricity.

Literally thousands of X-ray machines are used daily in medicine. Computerized tomography, commonly known as a CT or CAT scan, uses special X-ray equipment to make detailed images of bones and soft tissue in the body. Medical X-rays are the single largest source of man-made radiation exposure. Learn more about radiation sources and doses. X-rays are also used in industry for inspections and process controls.



The frequency of radiofrequency electromagnetic radiation ranges from **30 kilohertz (30 kHz, or 30,000 Hz) to 300 gigahertz (300 GHz, or 300 billion Hz)**. Electromagnetic fields in the radiofrequency range are used for telecommunications applications, including cell phones, televisions, and radio transmissions.

To put this in perspective, one should consider how much time that "smart" cell phone is in your hands or close proximity of your body. As China experienced resistance from the employees of Foxcon last year were in utter chaos because they were getting sick and dying from their work assembling the **5G** "smart" phones.

UK electrical engineers and energy weapons experts like Dr. Barry Trower and Mark Steele hold the professional opinion that **5G** "smart" phones are a military weapon. Mark Steele has become a famous anti-**5G** campaigner and activist. He is a British weapons expert and Chief Technology Officer, who stirred up quite a controversy in his hometown of Gateshead in Northern England. He became known in the media for the court case in Gateshead, sometimes referred to as "The Gateshead **5G** lamppost scandal".

He is now speaking internationally and giving lectures about the dangers and health effects of rolling out **5G** all over the world, and how it is all connected to a larger more sinister global government plan, part of a U.N. Agenda 21, New World Order depopulation plan. He calls **5G** a WEAPON TO KILL PEOPLE! He has been thoroughly investigating electromagnetic frequencies and radiation, and is now an expert on the topic, which has led media outlets and the local council to brand him as a "conspiracy theorist".

Mark Steele goes further in his investigation and is connecting the "man-made Climate Change CO2 scare" to **5G**, as a fraudulent billion Dollar control plan, and cover-up for not wanting to discuss the real agenda behind the roll-out of **5G**. He is also calling **5G** and the connection to A.I. – Artificial Intelligence, for a spiritual war.

Whatever one thinks of Mark Steele, the one thing that cannot be denied is the fact that **5G** technology can be and has been weaponized to deliver lethal doses of wireless energy through "beamforming". I posted recently an article on this topic and show how DEW or Directed Energy Weapons function and operate to reach anyone on the planet with the lethal dose of wireless energy. We know of people, government whistleblowers that have been subjected to wireless energy torture by our government

The article I posted on July 7, 2023 and is accessible at the link below:
Secret and Silent Frequency Wars

The facts suggested by Mark Steele and Dr. Barry Trower are further indication that the globalists plan to use **5G** weapons technology in their "Depopulation" program.

Even the FDA misleads the American public regarding the health risks of "Smart" cell phones.

How FDA Spins the Science on Cellphone Radiation and Human Health Risks

By Suzanne Burdick, Ph.D. | *The Defender* | July 7, 2023

Editor's note: *This is the first in a three-part series examining key questions in the public debate on the safety of wireless radiation. Part I addresses the question, How did the FDA arrive at its position on cellphones and cancer?*

The U.S. Food and Drug Administration (FDA) claims there's not enough scientific evidence to link cellphone use to health problems — but according to Devra Davis, Ph.D., MPH, a toxicologist and epidemiologist, the FDA's claim is untrue and misleading.

Davis spoke with *The Defender* about the important backstory leading up to the FDA's position on cellphone radiation as it relates to human health.

To support its statement — that "the weight of scientific evidence has not linked exposure to radio frequency energy from cell phone use with any health problems" — the FDA references a 2008-2018 literature review it conducted on radiofrequency (RF) radiation and cancer.

After completing the review, the FDA stated: "To date, there is no consistent or credible scientific evidence of health problems caused by the exposure to radio frequency energy emitted by cell phones."

However, Davis said the FDA's review was never signed. In other words, the names of the individuals who authored the report were never publicly released.

Davis has authored more than 200 peer-reviewed publications in books and journals, ranging from the *Lancet* to the *Journal of the American Medical Association*. She is the founding director of the Board on Environmental Studies and Toxicology of the U.S. National Research Council at the National Academy of Sciences and the founder and president of Environmental Health Trust.

Davis, who worked as a scientific adviser under multiple presidential administrations said, *"Normally, when you have a review at that high level it's quite consequential and it's always signed."*

"The reason it was unsigned, I believe," Davis told *'The Defender'*, "is because no one in the FDA was willing to put their name behind such a piece of junk. It was absolute nonsense," she said. *"It ignored many publications and only relied on an incredibly skewed interpretation of the literature — and I'm being generous when I say it like that."*

Davis pointed out that the FDA issued the review shortly after the **National Toxicology Program** (NTP) completed its multi-year $30 million study on cellphone radiation.

In that study, NTP researchers concluded there was "clear evidence" that male rats exposed to high levels of RF like that used in 2G and 3G cellphones developed cancerous heart tumors, and "some evidence" of tumors in the brain and adrenal gland of exposed male rats.

The NTP for decades has been the premier governmental testing program for pharmaceuticals, chemicals and radiation, said Davis, who served on the board of scientific counselors for the NTP when it was first started in the 1980s.

'Gold Standard' NTP study findings suppressed

Davis told *'The Defender'* that the government had access to a *"gold standard program testing with positive results"* that were consistent with and corroborated dozens of other studies. *"It wasn't like it [the NTP study] was a one-off study,"* she said.

Once the word got out that the findings of the NTP study were positive — meaning the government researchers had found an association between cellphone radiation and the growth of cancerous tumors — the telecommunication industry "started its tactics" to suppress the findings, Davis said.

Davis has been researching such tactics for more than a decade. This fall she plans to release a new edition of her 2010 book, *'**Disconnect**: The Truth About Cell Phone Radiation, What the Industry Is Doing to Hide It, and How to Protect Your Family.'*

Instead of the NTP study report being released in 2016 when it was first ready, she said, the **telecom industry** exerted pressure to subject the study's conclusions to an unprecedented level of scrutiny.

"When the first drafts began to circulate internally, it was elevated for a peer review unlike any that has ever been conducted in the history of the entire program — and I can say that with great certainty. No other compound or substance [studied by the NTP] has ever been subject to this level of peer review," Davis said.

A panel of external scientific experts convened for a three-day review of the study and its conclusions in March 2018.

However, rather than downplaying the study's conclusions, the experts concluded that the scientific evidence in the study was so strong that they recommended the NTP reclassify some of its conclusions from *"some evidence"* to *"clear evidence"* of carcinogenic activity.

Davis — who attended the three-day review — said, *"The reviewers that had been picked were people who were top-of-the-game toxicologists from Proctor and Gamble, from [Nokia] Bell Labs. [They were] industry toxicologists, but they were straight-up people."*

Davis said many of the experts spoke with her privately. *"The woman from Proctor and Gamble was concerned about her kids. She said, 'This [**cellphone radiation**] is not appropriate.' I said, 'Yes, that's what we've been trying to say for some time.'"*

More than 250 scientists — who together have published over **2,000 papers and letters** on the biologic and health effects of non-ionizing electromagnetic fields (EMFs) produced by wireless devices, including cellphones — signed the **International EMF Scientist Appeal**, which calls for health warnings and stronger exposure limits.

FDA rejects study it solicited, 'spins' it as faulty

When the experts' review of the NTP study was released, the FDA — which in 1999 requested the study and reviewed all its protocols, interim reports and final reports — the agency in November 2018, **repudiated the study** and in February 2020, released the **unsigned literature review** that criticized the study.

"They [the FDA] suddenly said, 'Well, the exposure chambers [used in the study] are not relevant to humans. The [radiation] levels were too high,'" Davis said. *"They were not."*

Davis was not alone in disagreeing with the FDA's rejection of the NTP study. More than 20 scientists, including Davis, wrote a **letter calling on the FDA** to retract the literature review. Many scientists **individually wrote** to the FDA as well.

Moreover, the Environmental Health Trust wrote a 188-page **report on the FDA's inaccuracies** in its research review and safety determinations about cellphone radiation.

Joel Moskowitz, Ph.D., director of the Center for Family and Community Health at the University of California, Berkeley, who has researched cellphone radiation for over a decade, identified nine "biased statements" made about the NTP study that *"tend to create doubt about data quality and implications."*

In *"**SPIN vs FACT:** National Toxicology Program report on cancer risk from cellphone radiation,"* Moskowitz lists and counters each statement. For example, Moskowitz noted that the claim the study's conclusions were faulty was rebutted by the **study report** itself.

Moskowitz also pointed out that **Christopher Portier, Ph.D.**, a retired head of the NTP who helped launch the study and still sometimes works for the federal government as a consultant scientist, told ***Scientific American***, *"This is by far — far and away — the most carefully done cell phone bioassay, a biological assessment."*

How telecom industry war-gamed study's results to manufacture doubt

According to Davis, the telecom industry has for decades influenced governmental agencies such as the FDA to *"manufacture doubt"* about scientific studies — such as the NTP study — that do not benefit it.

She pointed out that in the early 1990s, Motorola launched a *"**disinformation campaign** to confuse the public."* According to the Environmental Health Trust:

*"When first reports that cell phone radiation could damage DNA emerged from the laboratory of **Henry Lai** and **N.P. Singh** [both researchers at the University of Washington, Seattle] in the 90's, a memo written by Motorola to their media advisors in 1994 announced the clear strategy that remains alive and well: war-game the science."* The *"wargame"* memo — first released by ***Microwave News*** (see page 13) — showed that Norman Sandler of Motorola's corporate communications department on Dec. 13, 1994, wrote to Michael Kehs of the Burson-Marsteller public relations firm in Washington to plan how Motorola would respond to Lai and Singh's findings.

Sandler and Kehs had a three-point plan to impede further scientific research on how cellphone radiation might cause DNA damage and to create public doubt in such studies. The plan involved:

1. Delaying — or halting — Lai and Singh from continuing their DNA research.
2. Preventing other scientists from replicating the study, or carefully selecting scientists who would.
3. Convincing the press and the public using industry-selected scientists that the Lai-Singh DNA study results were of marginal importance and with questionable relevance in regard to the question of whether cellphones are safe for humans.

"I think we have sufficiently war-gamed the Lai-Singh issue, assuming SAG [the Scientific Advisory Group] and CTIA [the Cellular Telecommunications Industry Association] have done their homework," Sandler said.

Sandler said Motorola's executive vice president was "adamant" that the industry come up with a *"forceful one- or two-sentence portion of our standby statement that puts a damper on speculation arising from this research."*

Sandler proposed the industry say:

"While this work raises some interesting questions about possible biological effects, it is our understanding that there are too many uncertainties — related to the methodology employed, the findings that have been reported and the science that underlies them — to draw any conclusions about its significance at this time."

"That exact message," Davis said, *"keeps getting repeated and is well-funded to create doubts."*

She added:

*"The [telecom] industry has been very effective in their war games against science and scientists. We have to do a better job of clarifying the **science** and countering misleading and selective data from industry."*

The consumer needs to understand this technology is not without its downsize and in all cases the consumer has more to lose than to gain. DARPA, the CIA, and all the other intelligence gathering agencies hold the upper hand in this obsession to know everything there is to know about you, what you think, what you will do, how and where you spend your money, Your privacy and security means nothing to those in power.

Blessings,

Pastor Bob, EvanTeachr@aol.com
www.pastorbobreid.com