# NEWS

**A roundup of the latest Everyday News from the world of electronics**

## Watching you, watching me – Berlin report *by Barry Fox*

The Museum of Photography in Berlin is currently staging an exhibition, Watching Me, Watching You, which chronicles the history of surveillance – from early religious warnings that God's eye sees all, through the installation of sound funnels in the walls of the Louvre by French queen Catherine de Medici (1519–1589) to snoop on conversations of conspirators, to the modern use of high-resolution drone cameras.

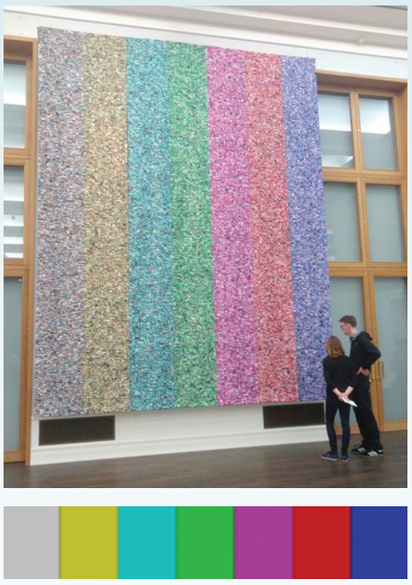
### Origins of modern snooping

Contemporary photos show how the military developed the sound funnel idea for locating planes in the pre-radar 1920s and 1930s. Systems consisted of pairs or quadrants of huge horns connected to stethoscope headphones by acoustic tubing.

The East German Stasi police took audio and photo surveillance to new heights, with a 1960 film camera so small that it could be concealed inside a cigarette lighter, and a system for automatically photographing post boxes with a telephoto lens to identify anyone who had posted a subversive letter. The Stasi also invested heavily in Polaroid cameras so that agents could take detailed photos of a home before searching it; so an untidy drawer or unmade bed looked exactly as it did before it had been gone through with a fine toothed comb.

The availability of digital cameras has made this technique far easier to employ. Until stopped under the Obama administration, the New York Police Department's Demographic/Zone Assessment Unit was monitoring the movement of Muslims living and working in the city.

One of the most most striking exhibits comes from Hasan Elahi, a mixed-race American who was



*(Top) Hasan Elahi's 30,000 pictures that document his movements over 12 year arranged in stripes to conform to the colour bars of the standard SMPTE TV test pattern (bottom).*

wrongly suspected by the FBI of terrorist activities and placed under surveillance. Elahi responded by taking digital photograph of every movement he made, in the street, around the house, in bathrooms and bedrooms, at home or when travelling, along with date, time and place metadata. Every week for the last 12 years he has sent the FBI many hundreds of these images. The total currently stands at 70,000 pictures.

For the Berlin exhibition he has collated 32,000 of these images, to construct a mural which groups the images in vertical stripes based on their predominant colour. The stripes conform to the colour bars of the standard SMPTE TV test pattern.

When I took a photo, I was told by a museum guard that no pictures of the surveillance exhibition were permitted – the irony escaped him.

### World War II bunkers

Across the city an organisation called the Berlin Underworld is now offering tours of recently discovered World War II underground bunkers and above-ground forts. Highlights include rabbit warrens of hidden rooms at some of the city's underground train stations. Air-lock doors, supposedly to protect against gas attack, were actually only cosmetic. For breathable air, the sealed shelters relied on shafts down to the underground train tracks, with the trains acting as piston pumps. If there had been a gas attack, the poison would have mixed with the air; but during raids the trains stopped running, so no air was pumped – but breathed-out carbon dioxide rose to poison levels.

In the pre-fax 1920s a pneumatic post system could send written messages across Berlin in minutes. This became a key comms system in WWII and was still being used in the city until the 1970s.

One of the underground shelter walls was painted with glow-in-the-dark phosphorescent paint. So the unfortunates packed inside during an air raid could still find their way to an Exit if the power was cut.

The original glow paint, applied in the 1940s, still retains some of its ability to store energy when illuminated and release it as light for up to 15 minutes in the subterranean darkness. Although this energy-efficient emergency lighting technique could appeal to modern architects, it cannot now be used in residential buildings because the world is more aware of the health risks in using chemicals such as zinc sulphide on walls that people may touch before eating with their fingers. In the war years this was a very secondary consideration.

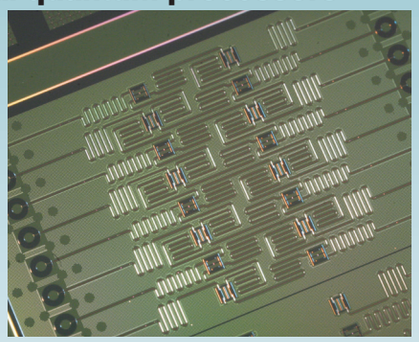
## IBM's most powerful universal quantum processors

IBM has announced two new powerful universal quantum computing processors. The first will be available for use by developers, researchers, and programmers to explore quantum computing using a real quantum processor – at no cost – via the IBM Cloud. The second is a new prototype of a commercial processor, which will be the core of the first IBM Q early-access commercial systems. IBM Q is an initiative to build commercially available universal quantum computing systems for business and science applications, delivered via the IBM Cloud platform.

The two IBM's devices are a 16- and 17-qubit processor. The 16-qubit processor allows more complex experimentation than the previously available 5-qubit processor. It is freely accessible to run quantum algorithms, enable work with individual quantum bits, and to explore tutorials and simulations.

The 17-qubit device is the most powerful quantum processor created to date by IBM and has been chosen to be the basis for the IBM Q early-access commercial systems.

'The significant engineering improvements announced will allow IBM to scale future processors to include 50 or more qubits, and demonstrate computational capabilities beyond today's classical computing systems,' said Arvind Krishna, senior vice president and director of IBM Research and Hybrid Cloud. 'These powerful upgrades to our quantum systems, delivered via the IBM Cloud, allow us to imagine new applications and new frontiers for discovery that are virtually unattainable using classical computers alone.'



*16-qubit processor, available for use by developers, researchers, and programmers to explore quantum computing using a real quantum processor via the IBM Cloud.*

Future applications of quantum computing may include:

- Business optimisation – improved solutions to problems found in supply chains, logistics, financial data modelling and risk analysis
- Materials and chemistry – untangling the complexity of molecular and chemical interactions to discover new materials and medicines
- Artificial intelligence – making facets of AI such as machine learning much more powerful
- Cloud security – using quantum physics to enhance the security of private data in the cloud.

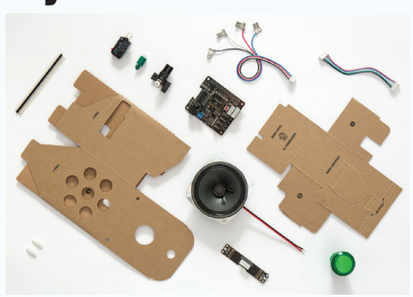
## Google uses Raspberry Pi for DIY AI

Google has launched 'AIY Projects', describing it as a route for constructors to do-it-yourself artificial intelligence or (artificial intelligence yourself, hence 'AIY').

The aim is for constructors to use artificial intelligence to make human-to-machine interaction more like human-to-human interactions. Google will be releasing a series of reference kits, starting with voice recognition. The speech recognition capability could be used to:

- Replace physical buttons and digital displays on household appliances and consumer electronics – imagine a coffee machine with no buttons or screen; you just talk to it
- Replace smartphone apps to control devices on connected devices such as a connected light bulb or thermostat – just talk to them
- Add voice recognition to assistive robotics (eg, for accessibility)

The kit includes a voice 'Hardware Accessory on Top' (HAT) that contains hardware for audio capture and playback; easy-to-use connectors for the dual mic daughter board and speaker; GPIO pins to connect low-voltage components like micro-servos and sensors; and an optional barrel connector for dedicated power supply. It was designed and tested with the Raspberry Pi 3 Model B.



*Google's AIY voice recognition kit*

The AI kit ships to subscribers of the *Raspberry Pi Magazine*, and will be on sale in the UK in WHSmith, Tesco and Sainsburys.

## IoT Power Calculator

Electronic component and equipment distributor Farnell has created an IoT Power Calculator that helps developers of IoT (Internet of Things) projects understand the expected battery life of their IoT devices, and allows them to experiment with different components and software algorithms to determine their impact on battery life.

Battery power is in increasing demand in IoT applications incorporating sensor systems that collect data and pass the information to the cloud. Unlike many larger connected systems, these relatively small devices often do not have access to mains power. This means that they must have a means of powering themselves, something that is achieved using either batteries or energy harvesting.

Although an increasing number of applications can now be developed at the ultra-low power levels required for energy harvesting, many more are not suitable for this approach, and in such cases batteries are needed.

The calculator is easy to use and very quick to produce a result. Users enter basic parameters about their hardware – including different types of microcontroller and batteries – and their software (how frequently the software wakes, and how many cycles the data capture/processing and communications operations require) and the calculator uses these inputs to work out the power consumption.

See: **http://uk.farnell.com/calculating-battery-life-in-iot-applications**

## Launch of Lorenz book

The fascinating autobiography by the late Capt Jerry Roberts has been launched at The National Museum of Computing. The book tells the story of the breaking of Hitler's most secret cipher.

The 'unbreakable' Lorenz cipher encrypted communications between Hitler and his high command. Far more complex than Enigma, Lorenz-encoded messages carried the most valuable strategic information.

Roberts' book gives an in-depth personal perspective of the breaking of the twelve-wheeled Lorenz cipher. One of the great intellectual achievements of the war, the Bletchley team assigned to crack Lorenz worked out how the machine operated without ever having seen it.

*Lorenz: Breaking Hitler's Top Secret code at Bletchley Park* by Jerry Roberts, The History Press, £20 (hardback), ISBN-13: 978-0750978859