Domino's to trial robots for pizza delivery

WELLINGTON: Fast food giant Domino's is to trial pizza delivery robots in New Zealand, it said yesterday, describing the hi-tech, driverless units as a world first. In a move enthusiastically backed by the New Zealand government, Domino's said it was working with authorities on plans to roll out its DRU (Domino's Robotic Unit).

The four-wheeler, developed in Australia, is just under a meter (three foot) high and contains a heated compartment that can hold up to 10 pizzas. It is battery powered and uses onboard sensors to avoid obstacles, with Domino's saying it can deliver pizzas within a 20 kilometer (12.5 mile) radius of a store before returning to recharge.

Customers are given a code when they order, which they enter onto a keypad to unlock the compartment containing their pizza. "DRU is cheeky and endearing and we are confident that one day he will become an integral part of the Domino's family," the chain's New Zealand general manager Scott Bush said. "He is a road to the future and one that we are very excited about exploring further."

While a date for the trial is yet to be finalized, Transport Minister Simon Bridges said the government working with Domino's on the project and was keen for it to proceed. "This is an exciting opportunity for New Zealand... over the last 12 months I've been actively and aggressively promoting New Zealand as a test bed for new transport technology trials," he said. New Zealand is still working on regulations relating to driverless vehicles such as the DRU, which is designed to operate on both roads and footpaths. — AFP

WELLINGTON: In a move enthusiastically backed by the New Zealand government, Domino's said it was working with authorities on plans to roll out its DRU (Domino's Robotic Unit). — AFP

ARLINGTON: In this file photo, President Barack Obama speaks at the National Cybersecurity and Communications Integration Center in Arlington, Virginia. — AP

Homeland Security begins sharing cyberthreats with business

WASHINGTON: The Homeland Security Department on Thursday formally began sharing details of new digital threats with private business and other government agencies, a culmination of a long-time effort to improve cybersecurity.

"This is the 'if you see something, say something' of cybersecurity," said Homeland Security Secretary Jeh Johnson at the agency's Virginia-based data sharing hub, the National Cybersecurity and Communications Integration Center.

A federal law passed at the end of 2015 was intended to encourage corporations to share information about cyberthreats, making it harder for businesses to be targeted by threats used elsewhere. The program is voluntary, and the number of companies that will participate or how effective the program will be remains unclear.

Companies have long been reluctant to acknowledge security failures. As of Thursday, about six organizations had signed up and others have expressed interest, Andy Ozment, the assistant cybersecurity secretary at Homeland Security, said. The names of companies participating are closely held, and records about their involvement are exempt from disclosure under the Freedom of Information Act. "This is a big deal," he said. "We're not going to launch out the gates ... and have thousands of companies sharing all sorts of information. We want to make sure we're providing value and growing."

Under the new law, the Homeland Security Department programmed its systems to remove personally identifiable information that might be included that private companies might share. "As companies come on board, we'll learn more about what's useful," and learn to streamline other parts, said Suzanne Spaulding, a top Homeland Security cyber official.

If information pertains to a specific threat of economic damage, death or serious injury or the effort to prosecute or prevent the exploitation of a minor, personal information may be passed on to other agencies. — AP

Apple-FBI fight may be the first salvo in a bigger war

SAN FRANCISCO: The Apple-FBI fight may just be the opening salvo in a broader war over encryption, as technology companies continue to lock up their users' messages, photos and other data to shield them from thieves and spies - and, incidentally, criminal investigators.

WhatsApp, the globally popular messaging system owned by Facebook, has already run into trouble on this front in Brazil. WhatsApp encrypts all user messages in 'end to end' fashion, meaning that no one but the sender and recipient can read them. Brazilian authorities arrested a Facebook executive earlier this month after the company said it couldn't unscramble encrypted messages sought by police. US officials are debating how to enforce a similar wiretap order for WhatsApp communications in a US criminal case, the New York Times reported . WhatsApp started as a way to exchange written messages over the Internet, but it has added services like photo-sharing and voice calling, while gradually building encryption into all those formats.

Spokesmen for WhatsApp and the Justice Department declined comment on the Times report, which said the wiretap order had been sealed to keep details secret. The Brazilian case is still pending, although the Facebook executive was released from jail after a day.

Legal battle

For now, US authorities and the tech industry are watching for the outcome of Apple's legal battle against the FBI, which wants to force the company to help unlock an encrypted iPhone used by one of the San Bernardino mass shooters. But as more companies explore adding encryption, further confrontations are likely.

"I think we can say, without a doubt, there is going to be more pressure on app-makers now," said Nate Cardozo, staff attorney at the Electronic Frontier Foundation. Cardozo said he is aware of other recent cases in which US authorities have approached individual companies that use encryption and warned them that criminals or terrorists are using their services. Cardozo declined to name the companies, but said authorities have urged those companies to "try harder" - by redesigning their apps or providing other technical solutions that would let agents read the encrypted messages.

Tech companies say they do not want to interfere with legitimate criminal investigations or national security matters. Instead, they argue they are concerned about criminal hacking, privacy invasion and violations of civil rights. "It is the government's job to protect public safety," said Denelle Dixon-Thayer, chief legal and business officer at Mozilla, which makes the Firefox Web browser. "Our job in the tech sector is to support that goal by providing the best data security."

Weakening encryption

While law enforcement authorities have chafed at tech companies' use of encryption, national security officials have warned against weakening encryption. "We are foursquare behind strong data security and encryption," Defense Secretary Ash Carter told a tech audience this month. He drew applause when he added, "I'm not a believer in back doors or a single technical approach to what is a complex problem."

Tech-industry encryption efforts expanded following 2013 disclosures by former National Security Agency contractor Edward Snowden that showed extensive government collection of Internet users' data. The resulting controversy helped spur companies like Apple, Google, Facebook and Yahoo to step up their security efforts, although the companies say they already had those plans in the works.

"There was a fundamental shift in relationships after the Snowden revelations," said Ed McAndrew, a former federal prosecutor now practicing law in Philadelphia, who said he has worked extensively with those companies on cybercrime investigations over the last decade. The companies felt "burned," he said, "so they decided to improve the privacy of their products."

One billion

WhatsApp, which boasts a billion users around the globe, first added encryption for its Android smartphone app in 2014. It has been gradually incorporating similar protections into other services, including messages sent on iPhones and even some voice calls. Founder Jan Koum traces his concerns about data-security stem to his parents' fear of government agents listening to phone calls in their native Ukraine. — AP