Θα Ενισχύσει το “Internet Of Things” τις Δυνατότητες της Επιτήρησης;

Chris Spannos
Μετάφραση: Στέφανος Μπατσής

Πόσο συχνά έχετε αφήσει ανοιχτή την πόρτα του ψυγείου, ψάχνοντας τι υπάρχει για να φάτε; Αυτή η δημοφιλής και εκ πρώτης όψεως αγαθή πράξη είναι μία μεταξύ πολλών άλλων που, σύμφωνα με τον Διευθυντή της Αμερικανικής Εθνικής Υπηρεσίας Πληροφοριών, James Clapper, μπορεί σύντομα να αναδειχτεί ως πηγή πληροφοριών που θα χρησιμοποιείται για τη διαχείριση και –αναμφισβήτητα– τον έλεγχο των πολιτών και των καταναλωτών.

Μέρος ενός κινήματος που αναφέρεται ως “Internet of Things” (IoT), το καινούριο «έξυπνο-ψυγείο» και ο «έξυπνος-φούρνος» της Samsung είναι τα τελευταία προϊόντα της σειράς «έξυπνο-σπίτι» που επιχειρούν να ενσωματώσουν όλες τις συσκευές, τις εφαρμογές, και τα αντικείμενα που χρησιμοποιούν αισθητήρες και δίκτυα πληροφοριών σε όλα τα σπίτια, τις επιχειρήσεις, τους χώρους εργασίας και τα αυτοκίνητα. Θεωρείται ότι θα αποτελέσει την επόμενη επανάσταση των υπολογιστών και προβλέπεται να αναδειχθεί σε μία βιομηχανία πολυ-τρισεκατομμυρίων δολαρίων μέσα στην επόμενη δεκαετία. Ωστόσο, αυτό που είναι άγνωστο σε πολλούς είναι ότι αυτά τα πράγματα μπορούν να μεταμορφωθούν σε μυστικές συσκευές παρακολούθησης.

«Στο μέλλον, οι μυστικές υπηρεσίες μπορεί να χρησιμοποιούν το IoT για ταυτοποίηση, επιτήρηση, παρακολούθηση, εντοπισμό τοποθεσίας και στρατολόγηση ή για να αποκτούν πρόσβαση σε δίκτυα ή πιστοποιήσεις χρηστών», ανέφερε ο Clapper σε δημόσια κατάθεση στην Αμερικάνικη Γερουσία την Τρίτη.

Η «έξυπνη-τηλεόραση» της Samsung έγινε γνωστή στο κοινό για την ικανότητά της να ακούει κρυφά τους χρήστες που μιλούσαν

μεταξύ τους, ενώ έβλεπαν την αγαπημένη τους εκπομπή. Εξίσου αβλαβή παιχνίδια, όπως η Barbie της Mattel που ενεργοποιείται μέσω Wi-Fi, μπορεί να χακαριστεί και να μεταμορφωθεί σε κούκλα κατάσκοπος κρυφακούγοντας προσωπικές συνομιλίες μεταξύ παιδιών, κουκλών και γονέων – οι οποίοι δεν γνωρίζουν ότι η ιδιωτικότητά τους παραβιάζεται. Με τον ίδιο τρόπο μπορούν να χρησιμοποιηθούν εσωτερικά μικρόφωνα σε αυτοκίνητα για να καταγράψουν κρυφά τους επιβάτες και να στείλουν τις συνομιλίες τους σε τρίτα μέρη.

Πολλές επιχειρήσεις –μεταξύ αυτών η Apple, η General Electric, η Nike και η Google– επενδύουν σε τεχνολογίες που θα συνδέουν καθημερινά αντικείμενα με το IoT και θα επεξεργάζονται τις πληροφορίες των χρηστών μέσα από υπηρεσίες cloud. Η αναμενόμενη αύξηση των δεδομένων που παράγονται από τους χρήστες έχει προκαλέσει ανησυχία στους ειδικούς για το ότι βαδίζουμε σε μία κλιμάκωση της επιτήρησης. Οι υπηρεσίες επιβολής του νόμου και οι μυστικές υπηρεσίες μπορεί να αρχίσουν να δίνουν εντολές στη Samsung, στη Google, ή σε πωλητές άλλων διαδικτυακών συσκευών, αναγκάζοντάς τους να επιβάλουν μια ενημέρωση ή να γυρίσουν έναν ψηφιακό διακόπτη για να υποκλέψουν τις προσωπικές συνομιλίες ενός στόχου.

Αυτές οι τάσεις ακολουθούν τις ήδη υπάρχουσες ανησυχίες για την κυβερνητική κατασκοπεία. Το 2013, ο πρώην ανάδοχος έργων της NSA (Εθνική Υπηρεσία Ασφάλειας), Edward Snowden, αποκάλυψε ότι η υπηρεσία των Η.Π.Α. και οι συνεργάτες της παρακολουθούσαν παράνομα πολίτες στο εσωτερικό και το εξωτερικό, καθώς και ότι κατασκόπευαν προέδρους και πρωθυπουργούς άλλων κρατών. Έκτοτε, διάφοροι ιδεολογικοί κύκλοι, ομάδες για τα ανθρώπινα δικαιώματα και πολίτες παγκοσμίως κρούουν τον κώδωνα του κινδύνου για την εξάπλωση της παράνομης συλλογής πληροφοριών μέσω της καταπάτησης της ιδιωτικότητας, των αστικών ελευθεριών και των ανθρωπίνων δικαιωμάτων.

Τον τελευταίο χρόνο, η Privacy International έχει αποκαλύψει παρακολουθήσεις στην Ουγκάντα, στο Πακιστάν, στην Κολομβία και

τη Σιγκαπούρη. Η Διεθνής Αμνηστία έχει προειδοποιήσει ότι οι κυβερνήσεις «σκουπίζουν» ηλεκτρονικά δεδομένα κάθε είδους και ότι η Βρετανική κυβέρνηση «είναι μεταξύ των βασικών ενόχων». Τον Δεκέμβρη, η PEN International επέδειξε σοβαρές ανησυχίες σχετικά με «τον υπερβολικό βαθμό ελέγχου που οι τουρκικές αρχές προσπαθούν να ασκήσουν πάνω σε νόμιμες, δημόσιες συνομιλίες στο διαδίκτυο». Στην Πολωνία, χιλιάδες συνειδητοποιημένοι πολίτες τον τελευταίο καιρό διαδηλώνουν κατά της κυβερνητικής επέκτασης των μέσων παρακολούθησης. Και τώρα ο Clapper προειδοποιεί σχετικά με τη χρήση του IoT για τη συλλογή πληροφοριών. Ο κόσμος είναι ανήσυχος.

Η επιτήρηση εγείρει πολλά πολιτικά και εθνικά προβλήματα. Χωρίς νομική κάλυψη, η παρακολούθηση στρεβλώνει τις δημοκρατικές αρχές και πρακτικές. Οι κυβερνήσεις υποστηρίζουν ότι είναι προς το συμφέρον της εθνικής ασφάλειας το να συλλέγουν κρυφά πληροφορίες από τους πολίτες. Έρευνες δείχνουν ότι οι ίδιες κυβερνήσεις επιθυμούν να έχουν πρόσβαση σε εταιρικούς λογαριασμούς ώστε να ψάχνουν τα αρχεία καταναλωτών. Ενώ ο κόσμος οικειοθελώς μοιράζεται και αποκαλύπτει προσωπικά στοιχεία για τους ίδιους, τις οικογένειες και τους φίλους τους στα μέσα κοινωνικής δικτύωσης κάθε μέρα, το Αμερικανικό Υπουργείο Άμυνας έχει μελετήσει εκτενώς πώς να επηρεάζει αυτούς τους χρήστες. Και το Facebook αμφιλεγόμενα ψάχνει να μάθει πώς να ελέγξει τα συναισθήματα των χρηστών με το να χειρίζεται τη ροή των ειδήσεών του.

Η κυβέρνηση και η επιχειρηματική δύναμη έχουν εξαπλωθεί μέσω των διαύλων της επικοινωνίας και της τεχνολογίας της πληροφορίας. Το “Internet of Things” θα επιτρέψει περαιτέρω αυτή την εξάπλωση μέσω της σύνδεσης των συσκευών. Όσο πιο πολύ οι αρχές υποκλέπτουν πληροφορίες από τους παρόχους υπηρεσιών και τις υπηρεσίες cloud, τόσο οι αθώες στιγμές της καθημερινότητας –το μαγείρεμα, η οδήγηση, το παιχνίδι, η χαλάρωση μπροστά από την τηλεόραση– θα γίνουν πλούσιες πηγές συλλογής πληροφοριών, που θα τροφοδοτούν τις κυβερνήσεις και τις εταιρείες σχετικά με τις προσωπικές επιλογές και

κοινωνικές συμπεριφορές, από τα πιο μικρά μέχρι και τα πιο μεγάλα. Με τόση πολλή τεχνολογία βέβαια, το ρίσκο βρίσκεται στο πώς θα εφαρμοστεί. Αν οι άνθρωποι είχαν προτεραιότητα, τέτοια δεδομένα θα μπορούσαν ιδανικά να τροφοδοτούν με πληροφορίες την κυβέρνηση και τις επιχειρήσεις, ώστε να προσπαθούν και να διασφαλίζουν μία περισσότερο δίκαιη κατανομή των πόρων. Τα ψυγεία θα μπορούσαν να μιλούν στους παραγωγούς σχετικά με την κατανάλωση φαγητού, παρέχοντας καλύτερες αξιολογήσεις ως προς τις ανάγκες και εξορθολογίζοντας την παραγωγή, ώστε να αποφευχθεί η σπατάλη. Όμως, στην αγορά του κεφαλαίου η χρήση της τεχνολογίας θα είναι να ωφελήσει τις ήδη πλούσιες επιχειρήσεις και να ενδυναμώσει την κρατική εξουσία. θα συνεχίσουμε να παραβλέπουμε την πείνα και τις ανάγκες εκείνων που δεν μπορούν να συμμετέχουν στην αγορά των προϊόντων στη σφαίρα του “Internet of Things”.

Μπορεί η κρυπτογράφηση να βοηθήσει στη μη συλλογή των πληροφοριών μας από αυτό το πλαίσιο – αυτό το οποίο ξεπερνάει αρκετά τα όρια του Μεγάλου Αδελφού του Τζορτζ Όργουελ; Όντως, ως απάντηση στην παράβαση της παρακολούθησης, οι πολίτες έχουν εφαρμόσει μια τεχνολογία κρυπτογράφησης στις επικοινωνίες τους. Ανταποκρινόμενες στις ανάγκες της αγοράς, κάποιες μεγάλες εταιρείες, όπως η Apple, η Google και το Facebook, έχουν αναπτύξει υπηρεσίες και προϊόντα που παρέχουν τη δυνατότητα της κρυπτογράφησης, όπου δεν υπάρχει κανένα άτομο στη μέση που να μπορεί να κρυφακούει τις επικοινωνίες κάποιου χρήστη.

Η αυξανόμενη χρήση της κρυπτογράφησης, υποβοηθούμενη από μεγάλες εταιρείες που παρέχουν επιλογές για ασφαλείς επικοινωνίες, έχει ανησυχήσει κυβερνητικούς αξιωματούχους. Στις ΗΠΑ, το FBI, η CIA και η NSA έχουν εδώ και καιρό παραπονεθεί ότι «βυθίζονται στο σκοτάδι», όπου το κενό μεταξύ της κυβερνητικής εξουσίας και της τεχνολογικής δυνατότητας για τη συλλογή πληροφοριών διευρύνεται.

Σε μία πρόσφατη έρευνα που δημοσιεύτηκε από το Πανεπιστήμιο του Harvard, ειδικοί στην παρακολούθηση και τη διαδικτυακή

ασφάλεια παραθέτουν ότι οι επικοινωνίες κινούνται σταθερά πέρα από το εύρος του κυβερνητικού ελέγχου. Η κυβέρνηση εκφράζει φόβους πως ένα «άνοιγμα κλείνει» και, εφόσον κλείσει, θα είναι πλέον «τυφλοί». Ωστόσο, οι ειδικοί δεν συμφωνούν, δηλώνοντας ότι η μεταφορά του «βυθίζονται στο σκοτάδι», «δεν αποτυπώνει την παρούσα κατάσταση και την πορεία της τεχνολογικής ανάπτυξης».

Όπως έχει αναγνωριστεί από τους ειδικούς, οι περισσότερες εταιρείες είναι απίθανο να υιοθετήσουν τεχνολογίες κρυπτογράφησης. Οι περισσότερες μπορούν να εξαργυρώσουν ήδη συλλεγμένες πληροφορίες με το να πωλούν στοχευμένες διαδικτυακές διαφημιστικές ευκαιρίες. Στην πραγματικότητα, η πλειοψηφία των επιχειρήσεων που παρέχουν υπηρεσίες επικοινωνίας βασίζονται στην πρόσβαση των δεδομένων του χρήστη για τα έσοδα και τη λειτουργικότητα του προϊόντος. Τα λογισμικά οικοσυστήματα έχουν την τάση να είναι ευάλωτα, γεγονός που μπορεί να καταστήσει τη διαδεδομένη χρήση της τεχνολογίας της κρυπτογράφησης δύσκολη. Πολλές από τις εταιρείες που παρέχουν επιλογές κρυπτογράφησης, παρέχουν εξίσου πληροφορίες στις κυβερνήσεις, οι οποίες μπορούν να χρησιμοποιηθούν για παρακολούθηση.

Το IoT θα αλλάξει το περιβάλλον και τον προσωπικό μας χώρο. Αυτές οι αλλαγές θα παρέχουν περισσότερες δυνατότητες για παρακολούθηση. Η ιδιωτικότητα χάνεται. Η επιτήρηση θα ξεπεράσει (όπως έχει εδώ και καιρό ξεπεράσει) τους ισορροπημένους στόχους της εθνικής ασφάλειας. Παρ’ όλα αυτά, πολλοί θα επηρεαστούν από τους ισχυρισμούς της κυβέρνησης να αυξήσει την επιτήρηση για τη δική μας προστασία. Ενώ η IoT επανάσταση υπόσχεται άνεση και ευκολία, είμαστε πρόθυμοι να παρέχουμε στις κυβερνήσεις και τις εταιρίες ακόμη περισσότερες προσωπικές πληροφορίες σε μία παράλληλη επανάσταση παρακολούθησης που θα κλιμακώσει τη διαχείριση και τον έλεγχο των ανθρώπων και της κοινωνίας;

*Ο **Chris Spannos** είναι Αμερικάνος ακτιβιστής, δημοσιογράφος, συγγραφέας, εκδότης, παραγωγός και web developer με πάνω από 18 χρόνια εμπειρίας σε αυτοδιαχειριζόμενα media. Συντάκτης της ηλεκτρονικής πλατφόρμας New Internationalist Magazine και του teleSUR English καθώς και παλαιότερα του NYTimes eXaminer και του Imaginary Lines. Μέλος του αμερικανικού δικτύου ZNet και ZCom. Εχει εκδόσει το βιβλίο Real Utopia: Participatory Society for the 21st Century (AK Press, 2008). Εχει συνεισφέρει κεφάλαια σε βιβλία όπως το The Accumulation of Freedom (AK Press, 2012) και το The End of the World as We Know It (AK Press, 2014). Βρίσκεται μεταξύ των φετινών ομιλητών του B-FEST.*

Πηγή:
https://newint.org/blog/2016/02/11/will-the-internet-of-things-boost-surveillance-capabilities/

Περιοδικό Βαβυλωνία #Τεύχος 18