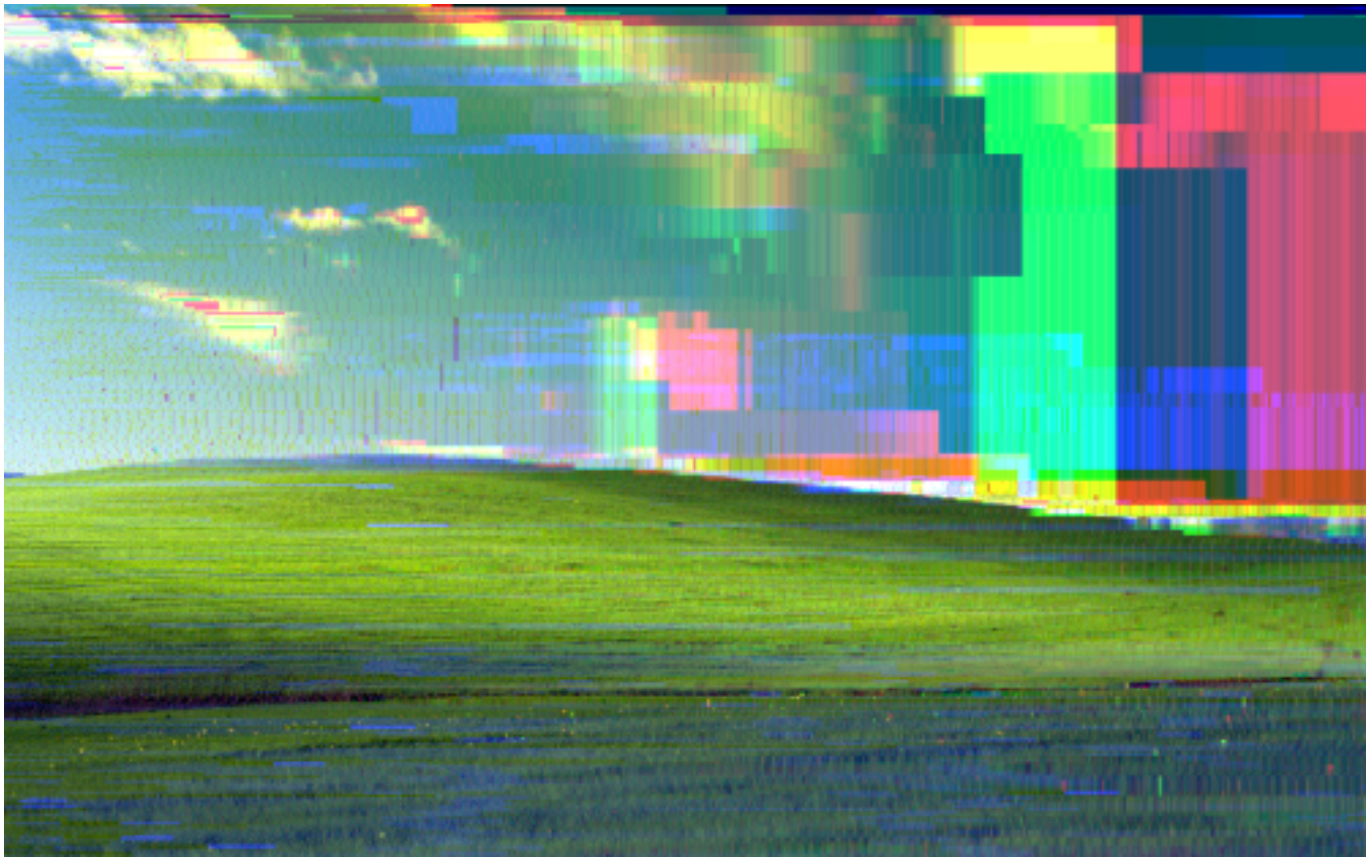
Υποκλοπές e-mail – Τι έμαθα στο Coursera (εβδομάδα 3α)



Προηγούμενες αναρτήσεις από το μάθημα Surveillance Law του Coursera:
Νομοθεσία των ΗΠΑ περί παρακολουθήσεων (εβδομάδα 1)
Τηλεφωνικές παρακολουθήσεις εντός ΗΠΑ (εβδομάδα 2)

Υποκλοπές με τις νέες τεχνολογίες

Το πρόβλημα του να προσπαθείς να εφαρμόσεις συνταγματικές και νομοθετικές προβλέψεις που συντάχθηκαν προ 50ετίας για να ρυθμίσουν τις τηλεπικοινωνίες στα δεδομένα των νέων τεχνολογιών, αναδεικνύεται σε όλο του το μεγαλείο στις κρατικές παρακολουθήσεις που αφορούν διαδικτυακές επικοινωνίες. Οι αντιστοιχίσεις αναλογικών καταστάσεων με τις

νέες, ψηφιακές, συχνά ακούγονται λογικές. Δεν ακούγεται παράλογο π.χ. το να λέγεται ότι πρέπει να ισχύει για τα τσατ (instant messaging) ό,τι προβλέπεται για μια τηλεφωνική συνομιλία με σταθερό, ή ότι το να παραβιάζεις ένα password είναι σαν να εισβάλεις στο σπίτι κάποιου. Αλλά στην πράξη, για τους αμερικανούς νομοθέτες και δικαστές, η προστασία της ιδιωτικότητας στο ίντερνετ δεν είναι τόσο αυτονόητη.

E-mail και instant messaging

Το πότε και σε ποιο βαθμό η ηλεκτρονική αλληλογραφία ενός κατοίκου των ΗΠΑ μπορεί να εκτίθεται στα μάτια των αρχών, καθορίζεται ουσιαστικά από την ομοσπονδιακή νομοθεσία που καθορίζει πότε οι αμερικανικές αρχές μπορούν να έχουν πρόσβαση στους σέρβερ μιας εταιρείας που παρέχει υπηρεσίες e-mail (π.χ. της Google, για κάποιον που έχει @gmail) και στα δεδομένα και τις πληροφορίες που αυτή η εταιρεία διατηρεί για τους πελάτες της.

Ο νόμος διαχωρίζει υποκατηγορίες δεδομένων που συλλέγει η εταιρεία e-mail για κάθε πελάτη, οι οποίες τυγχάνουν διαφορετικής αντιμετώπισης. Ένα βασικό κριτήριο διαχωρισμού τους είναι το αν αυτά έχουν ήδη συλλεχθεί (**retrospective data collection**) ή αν πρόκειται να συλλεχθούν στο μέλλον (**prospective data collection**):

• Στην κατηγορία **αναδρομικών συλλογών δεδομένων/πληροφοριών** υπάρχουν τέσσερις υποκατηγορίες:
– **πληροφορίες λογαριασμού** του πελάτη (π.χ. όνομα, διεύθυνση) που διαθέτει η εταιρεία
– **μεταδεδομένα από τις ήδη πραγματοποιημένες συνδέσεις του πελάτη στον λογαριασμό του e-mail του**, τις υπηρεσίες που χρησιμοποίησε από τη στιγμή που έκανε log-in, το δίκτυο από το οποίο συνδέθηκε, τη διάρκεια την σύνδεσης κ.α. (δεν περιλαμβάνονται δεδομένα από το περιεχόμενο των επικοινωνιών του)

– **μεταδεδομένα των μηνυμάτων** που ήδη αντάλλαξε (π.χ. ποιοι είναι οι παραλήπτες, χρόνοι αποστολής, μέγεθος μηνυμάτων)
– **περιεχόμενο των μηνυμάτων** που έχει ανταλλάξει (θέμα και σώμα του μηνύματος)

• Στην κατηγορία **μελλοντικών συλλογών δεδομένων/πληροφοριών** υπάρχουν οι ίδιες υποκατηγορίες, πλην των πληροφοριών λογαριασμού:
– **μεταδεδομένα των μελλοντικών συνδέσεων** του πελάτη στον λογαριασμό του e-mail του
– **μεταδεδομένα των μηνυμάτων** που θα ανταλλάξει
– **περιεχόμενο των μηνυμάτων** που θα ανταλλάξει.

Διαδικασίες εξασφάλισης πρόσβασης σε μελλοντικά e-mail

Η πρόσβαση σε μελλοντικά e-mail καθορίζεται από το **Νόμο περί Υποκλοπών (Wiretap Act)** ή από τον SCA, ανάλογα με το τι θέλουν να δουν οι αρχές. Για να αποκτήσουν πρόσβαση στο περιεχόμενο ενός e-mail χρειάζονται **ένταλμα**, αλλά για πρόσβαση στα υπόλοιπα (μεταδεδομένα συνδέσεων και κλήσεων, που όλα μαζί, εν συντομία, αποκαλούνται **DRAS** από τα “dialing,routing, addressing, signaling”],) αρκεί μια **εντολή καταγραφής/παγίδευσης (Pen/Trap order)**.

Διαδικασίες εξασφάλισης πρόσβασης σε παλιά e-mail

Η νομοθεσία που οριοθετεί την πρόσβαση των αρχών στα ήδη απεσταλμένα ή παραληφθέντα e-mail των πολιτών μοιάζει πολύ σε αυτή για τις ήδη **πραγματοποιημένες τηλεφωνικές κλήσεις**. Καθορίζεται από το **Νόμο περί Αποθηκευμένων Επικοινωνιών (Stored Communications Act, εν συντομία SCA)***.

Όπως και με τις τηλεπικοινωνίες, για να έχουν πρόσβαση οι αρχές στα **στοιχεία λογαριασμού** του πελάτη (του κατόχου ενός e-mail στη συγκεκριμένη περίπτωση) αρκεί μια κλήτευση προς την εταιρεία. Αν ο αστυνομικός βεβαιώσει γραπτώς ένα δικαστή ότι

τα στοιχεία που θέλει να δει σχετίζονται με κάποια έρευνα, ο δικαστής είναι υποχρεωμένος να εγκρίνει την κλήτευση. Ο πελάτης δεν θα μάθει ποτέ ότι η αστυνομία εξασφάλισε πρόσβαση στα δεδομένα του. Το ίδιο ισχύει και για τα **μεταδεδομένα των συνδέσεων** που πραγματοποίησε στο e-mail του.

Όσο για το **περιεχόμενο των μηνυμάτων**, χρειάζενται ένταλμα, όπως συμβαίνει και με το περιεχόμενο των τηλεφωνικών κλήσεων (βάσει του Wiretap Act).

Υπάρχει, όμως και μια κατηγορία δεδομένων που δεν θεωρείται ούτε περιεχόμενο, ούτε πληροφορίες λογαριασμού ή μεταδεδομένα κλήσεων και συνδέσεων, το «**μη-περιεχόμενο**» που δεν τυγχάνει της ίδιας προστασίας. Σε αυτή την κατηγορία κατατάσσονται τα **μεταδεδομένα των μηνύματων (αποστολέας, παραλήπτης, ώρα, διάρκεια)**.

Για την πρόσβαση στο «μη-περιεχόμενο» των e-mail εφαρμόζεται ένας νέος τύπος δικαστικής εντολής, η **D-order**, που λειτουργεί ως μίνι-ένταλμα. Δεν απαιτεί από τον αστυνομικό να αποδείξει πολλά πράγματα στον δικαστή για να αιτιολογήσει την ανάγκη παραβίασης της ιδιωτικότητας του κατόχου του e-mail. Αρκεί να ικανοποιείται το **"πρότυπο RAS"** (**Reasonable Articulable Suspicion standard**), που είναι κάτι περισσότερο από το να επικαλεστεί απλώς «σχετικότητα» (relevance) με την υπόθεση, αλλά είναι κάτι λιγότερο από το να τεκμηριώσει «πιθανή αιτία» (probable cause ή PC). Για να καταλάβει κανείς πώς λειτουργεί το πρότυπο RAS, μπορεί να φανταστεί έναν αστυνομικό που σταματάει ένα αυτοκίνητο για έλεγχο σε ένα δρόμο των ΗΠΑ. Το κάνει βάσει του ίδιου προτύπου, που του δίνει το δικαίωμα να ακινητοποιεί κάποιον βάσει μια απλής υποψίας (αλλά όχι απλής διαίσθησης ή ανώνυμης πληροφορίας), που να βασίζεται σε κάποιου είδους απόδειξη (όχι σαφώς προσδιορισμένη).

Σε καμμία περίπτωση δεν προβλέπεται ότι ο κάτοχος του e-mail θα ενημερωθεί για την πρόσβαση των αρχών σε οποιοδήποτε από τις κατηγορίες δεδομένων του. Επιπλέον, ακόμη κι αν κατά την εκδίκαση μιας υπόθεσης διαπιστωθεί ότι οι αρχές βασίστηκαν σε

παράνομες υποκλοπές πληροφοριών παραβιάζοντας τις διατάξεις του νόμου SCA, δεν επιτρέπεται να ζητηθεί από το δικαστήριο να μην τις χρησιμοποιήσει (“suppression”).

E-mail που ανοίχτηκαν ή έμειναν αποθηκευμένα πάνω από 180 μέρες

Κάτι που μάλλον αγνοούν οι περισσότεροι χρήστες, είναι ότι **υπάρχουν δύο κατηγορίες e-mail που εξαιρούνται από την προστασία του νόμου και δεν χρειάζεται ούτε καν D-order, αλλά μια απλή κλήτευση για να τεθούν στη διάθεση των αρχών**:

– **μηνύματα που έχουν αποθηκευτεί σε κάποιο σέρβερ για πάνω από 180 μέρες** και
– **μηνύματα που έχουν ανοιχτεί** για να διαβαστούν.

Στις περιπτώσεις αυτές, ωστόσο, ο κάτοχος του λογαριασμού πρέπει να ειδοποιηθεί για την παρακολούθησή του.

Στην πρώτη περίπτωση θεωρείται ότι το ένα μήνυμα που αφέθηκε χωρίς να διαγραφεί επί 180 μέρες, είναι εγκαταλειμμένο, άρα δεν χρειάζεται προστασία. Αυτή η λογική, βέβαια, αντανακλά μια παλιά λογική διαχείρισης μηνυμάτων, που δεν εφαρμόζεται από τότε που έγιναν διαθέσιμη η αποθήκευση σε cloud, που αφορά πλέον την τεράστια πλειοψηφία των επικοινωνιών. Ωστόσο, ο νόμος ισχύει.

Στη δεύτερη περίπτωση, η εξαίρεση βασίζεται σε μια ερμηνεία του Υπουργείου Δικαιοσύνης των ΗΠΑ, που έκρινε κάποια στιγμή ότι από τη στιγμή που θα ανοιχτεί ένα μήνυμα δεν είναι ούτε «προσωρινά» αποθηκευμένο, ούτε αποτελεί «backup». Η προστασία που παρέχει ο νόμος SCA και επιβάλει έκδοση εντάλματος, ισχύει μόνο για επικοινωνίες «προσωρινά αποθηκευμένες» (δηλαδή όσο τα μηνύματα μένουν στους σέρβερ της εταιρείας, στη φάση που αυτή λειτουργεί μόνο ως αγωγός επικοινωνίας και όχι ως παραλήπτης της) ή αποθηκευμένες ως «αντίγραφα ασφαλείας». Δεν συμφωνούν όλα τα δικαστήρια με αυτή την ερμηνεία. Κάποια την

αποδέχονται, άλλα την απορρίπτουν, ενώ υπάρχει και μια ενδιάμεση ερμηνεία, που αποδέχεται ότι είναι προστατευμένα τα μηνύματα που έχουν ανοιχτεί αν ο χρήστης έχει κατεβάσει και κάποιο αντίγραφό τους στον υπολογιστή του.

Και μια τεχνική λεπτομέρεια: **Οι αρχές δεν πραγματοποιούν με δικά τους μέσα τις υποκλοπές** από τους σέρβερ όπου είναι αποθηκευμένα τα μηνύματα. Μεταβιβάζουν τα εντάλματα, τις D-order και τις κλητεύσεις στις εταιρείες που παρέχουν υπηρεσίες e-mail στους υπό παρακολούθηση, οι οποίες συλλέγουν τα δεδομένα ή/και τα μεταδεδομένα που ζητήθηκαν και τους τα στέλνουν.

Η εμπλοκή της Τέταρτης Τροποποίησης του Συντάγματος στη συλλογή πληροφοριών από παλιά e-mail

Μέρος του Νόμου περί Αποθηκευμένων Επικοινωνιών έχει κριθεί πλέον αντισυνταγματικό και, αυτό έχει κάποιες επιπτώσεις σε σχετικές υποθέσεις. Κι αυτό συμβαίνει γιατί πολλά δικαστήρια άρχισαν να αμφισβητούν το «**δόγμα τρίτου μέρους**», δηλαδή την αντίληψη ότι δηλαδή οι χρήστες εκχωρούν οικειοθελώς τα δεδομένα τους στις εταιρείες, συνεπώς αυτά δεν είναι απόρρητα. **Σήμερα**, (μετά από μια **δευτεροβάθμια δικαστική απόφαση του 2010** που δεν έχει αμφισβητηθεί ακόμα), **θεωρείται πως το περιεχόμενο των μηνυμάτων ηλεκτρονικού ταχυδρομείου προστατεύεται από το αμερικανικό Σύνταγμα**, όταν δεν υπάρχουν άλλες εξαιρέσεις (όπως οι παραπάνω).

Η προστασία αφορά και μηνύματα που αποθηκεύουμε μέσω των υπηρεσιών της εταιρείας που μας παρέχει το e-mail, καθώς κρίθηκε πως η αποθήκευση των μηνυμάτων σε ένα σέρβερ είναι κάτι σαν να νοικιάζαμε ένα φυσικό χώρο για να φυλάξουμε κάτι ή σαν να κλείνουμε ένα δωμάτιο ξενοδοχείου (ιδιωτικοί χώροι που χαίρουν συνταγματικής προστασίας στις ΗΠΑ).

Μετά από αυτή την απόφαση, η αστυνομία δεν μπορεί να παρουσιάσει σε κάποιο δικαστήριο αποδεικτικά στοιχεία που

άντλησε από το περιεχόμενο ενός e-mail αν τα πήρε χωρίς ένταλμα. Επιπλέον, θεωρείται πιθανό η συγκεκριμένη απόφαση να χρησιμοποιηθεί για να αντικρούσει στο μέλλον παρακολουθήσεις που βασίστηκαν στις εξαιρέσεις περί 180 ημερών ή ανοιχτών μηνυμάτων.

Προσδιορισμός των ορίων των ενταλμάτων που αφορούν αποθηκευμένες συνομιλίες

Τα δικαστήρια διαφωνούν για τους προσδιορισμούς των ορίων (particularity) που πρέπει να τίθενται στις παρακολουθήσεις μηνυμάτων ηλεκτρονικού ταχυδρομείου. Η σχετική πρόβλεψη που υπάρχει για κάθε ένταλμα (και εφαρμόζεται στις τηλεφωνικές υποκλοπές), είναι ότι **η παρακολούθηση θα περιορίζεται στο κομμάτι των επικοινωνιών που αφορά την υπόθεση που διερευνάται**, και ότι θα αγνοούνται π.χ. άσχετες οικογενειακές συνομιλιές.

Στα εντάλματα που αφορούν e-mail, τα δικαστήρια δεν ακολουθούν όλα την ίδια τακτική που θα ήταν αναμενόμενη κατ'αναλογία. Άλλα θέτουν τέτοιους περιορισμούς για να εκδόσουν εντάλματα, άλλα παραπέμπουν σε φιλτράρισμα που πρέπει να κάνουν οι εταιρείες e-mail κι άλλα το αφήνουν στους αστυνομικούς να κάνουν το φιλτράρισμα. Ορισμένα δικαστήρια μάλιστα, αγνοούν την ανάγκη τέτοιου προσδιορισμού και επιτρέπουν την πρόσβαση σε όλα τα e-mail του παρακολουθούμενου, μέχρι να βρουν οι αστυνομικοί ό,τι χρειάζονται για την έρευνά τους, ρισκάροντας έτσι μια παραβίαση της Τέταρτης Τροποποίησης του συντάγματος.

Επόμενες αναρτήσεις:

Πλοήγηση στον Ιστό, υποκλοπές από κινητά και κυβερνητικό χάκινγκ (εβδομάδα 3β)

Εξαναγκασμός εταιρειών και ατόμων να συνεργάζονται στις κρατικές παρακολουθήσεις (εβδομάδα 4)

Παραπομπή

* **Νόμος περί Αποθηκευμένων Επικοινωνιών (Stored Communications Act, εν συντομία SCA)**, του 1986. Ρυθμίζει πότε οι ομοσπονδιακές αρχές μπορούν να έχουν αναδρομική πρόσβαση τόσο στις πληροφορίες λογαριασμών ενός πελάτη μιας εταιρείας τηλεπικοινωνιών/e-mail, όσο και στις ίδιες τις επικοινωνίες (κλήσεις, συνομιλίες, e-mail κλπ) που έχουν ήδη γίνει. Σύμφωνα με τον SCA ο πάροχος μιας υπηρεσίας επικοινωνίας οφείλει να αποκαλύπτει στην κυβέρνηση:

α. το όνομα

β. τη διεύθυνση

γ. τα αρχεία τοπικών και υπεραστικών τηλεφωνικών συνδέσεων, ή τα αρχεία τως ωρών των συνδέσεων και της διάρκειάς τους

δ. τη διάρκεια της υπηρεσίας (συμπεριλαμβανομένης της στιγμής έναρξης) και τα είδη υπηρεσιών που παρασχέθηκαν

ε. τον αριθμό ταυτοποίησης της τηλεφωνικής ή άλλης συσκευής που χρησιμοποιήθηκε ή άλλο αριθμό καταγραφής και ταυτοποίησής του συνδρομητή, συμπεριλαμβανομένης κάθε προσωρινής διεύθυνσης σύνδεσης στο ίντερνετ, και

στ. τα μέσα και της πηγές μέσω των οποίων πληρώθηκε η υπηρεσία (συμπεριλαμβανομένης τυχόν πιστωτικής κάρτας ή τραπεζικού λογαριασμού) του πελάτη που χρησιμοποίησε την υπηρεσία [κατόπιν κλήτευσης στο πλαίσιο έρευνας]. Δεν υπάρχει καμμία υποχρέωση του κρατους ή της εταιρείας να ενημερώσει τον πελάτη ότι όλα αυτά τα στοιχεία των επικοινωνιών του κοινοποιήθηκαν στις αρχές.