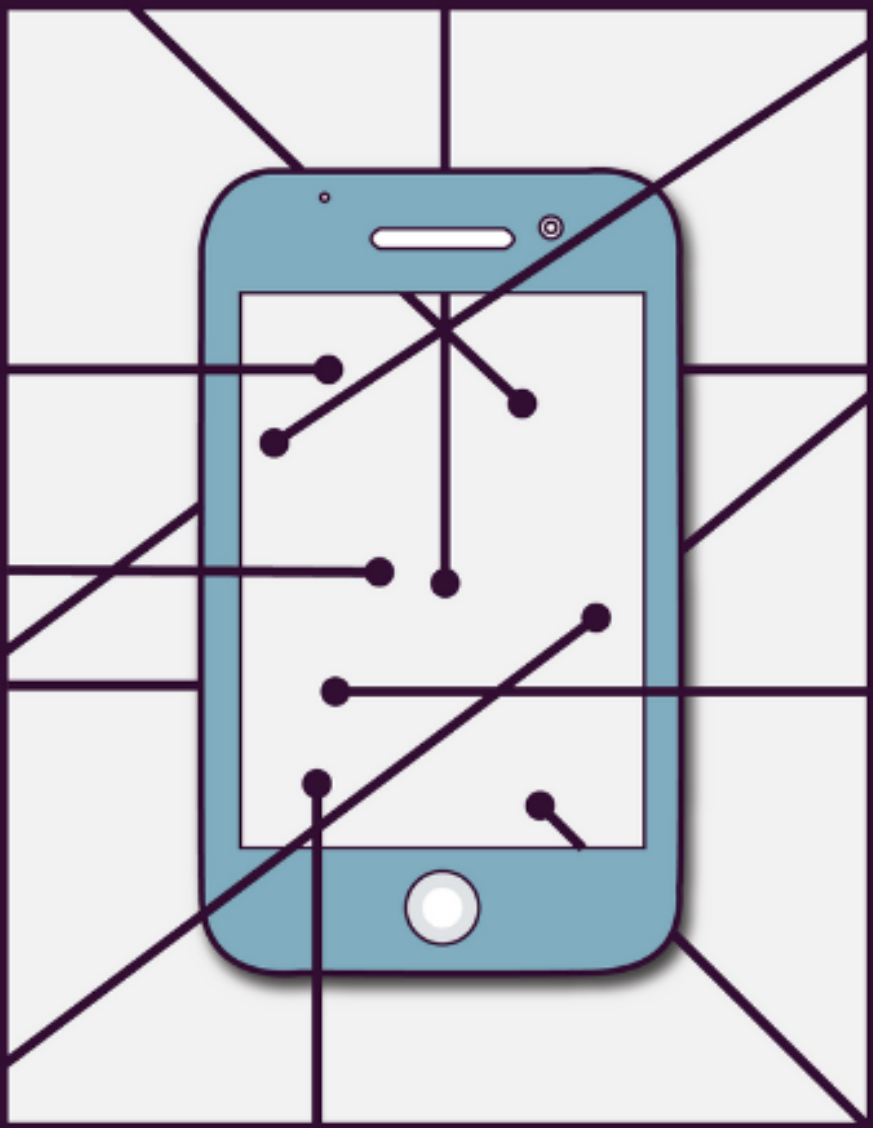
Buod na Bersyon ng Mga E-Device

Ang Iyong Mga Karapatan sa Digital Privacy sa Border



BC CLA

CIPPIC

Buod na Bersyon ng Mga E-Device

Ang Iyong Mga Karapatan sa Digital Privacy sa Border

Ang gabay na ito ay magbibigay sa iyo ng impormasyon tungkol sa iyong mga karapatan sa privacy pagdating sa iyong mga device – gaya ng mga laptop, cellphone, at tablet – sa border. Ginawa ito para sa mga taong tumatawid sa border upang pumasok sa Canada o pumunta sa U.S. sa pamamagitan ng mga lugar naa preclearance sa Canada.

Kadalasan, hindi maaaring random na magsagawa ang pulisya ng pagsisiyasat kung wala silang hinala, ngunit hindi ganito ang kaso sa border. Ang *Charter of Rights and Freedoms* ay ginagamit sa border, ngunit napagpasyahan ng mga hukuman na bigyan ng higit na kapangyarihan ang CBSA na siyasatin ang mga indibidwal at ang kanilang mga kagamitan kaysa sa mga pulis sa ibang lugar, dahil na rin sa kagustuhan ng pamahalaang pigilan ang pagpasok ng mga mapanganib na produkto at hindi kanais-nais na indibidwal sa bansa.

Binibigyan ng *Customs Act* ang Canadian Border Services Agency (CBSA) ng kapangyarihang siyasatin ang mga tao at produktong pumapasok sa bansa, kasama ang kanilang mga dalang kagamitan. Kabilang dito ang nilalaman ng – ang mga file, larawan, at video sa – iyong mga digital na device. Ang mga file sa iyong mga device ay "mga produkto" sa ilalim ng *Customs Act*, at maaaring siyasatin ng mga opisyal sa border ang mga produktong pumapasok sa Canada nang walang warrant – kahit wala silang dahilan upang paghinalaang kontrabando o naglalaman ng kontrabando ang mga naturang produkto.

Maaari ring siyasatin ang mga hindi mamamayang gustong pumasok sa Canada, kasama ang mga asylum seeker. Sa ilalim ng *Immigration and Refugee Protection Act*, maaaring siyasatin ng isang opisyal ng CBSA ang bagahe at mga personal na kagamitan ng isang taong gustong pumasok sa Canada sa isang port of entry, kasama ang mga electronic na device at media. Gayunpaman, dapat ay:

- makatuwiran ang dahilan ng opisyal sa paniniwalang hindi ibinunyag ng indibidwal ang kanyang pagkakakilanlan, o na may mga itinago siyang dokumentong nauugnay sa pagiging kwalipikado niyang pumasok sa bansa, o
- makatuwiran ang dahilan ng opisyal sa paniniwalang nauugnay ang indibidwal sa pagpupuslit ng mga tao o people smuggling, pangangalakal ng tao o human trafficking, o pamemeke ng dokumento.

Dapat limitahan ang mga pagsisiyasat ng mga device sa pagtukoy sa pagkakakilanlan ng indibidwal, paghahanap ng mga dokumentong nauugnay sa pagiging kwalipikado niyang pumasok sa bansa, o katibayan ng mga paglabag na nakabalangkas sa itaas.

Mga Paunang Pagsisiyasat

Paunang sisiyasatin ng mga front-line officer ang mga nilalaman ng iyong device sa pamamagitan ng pag-browse sa mga larawan, video, at file. Isa itong mabilisang pagtingin sa mga nabanggit na nilalaman upang matiyak na hindi naglalaman ang mga ito ng kontrabando – gaya ng pornograpiya ng bata o nakapopootna lathalain – o katibayan ng isang krimen. Maaaring random o may target ang mga paunang pagsisiyasat.

Kahit na sino ay maaaring isailalim sa isang random na pagsisiyasat. May mga nagsasabing tina-target ang mga manlalakbay batay sa kanilang lahi o relihiyon, at na maaaring magpanggap ang mga opisyal na isang "random" na pagsisiyasat ang isinasagawa nilang profiling. Bagama't labag sa batas ang anumang

uri ng profiling, mahirap patunayang diskriminasyon nga ito. Kung sa palagay mo ay nakaranas ka ng diskriminasyon, makakakita ka ng higit pang impormasyon tungkol sa paghahain ng reklamo sa ibaba.

Hindi random na napili ang karamihan sa mga taong sinisiyasat ng CBSA, sa halip, napili sila sa pamamagitan ng pag-target. Tina-target ang mga tao batay sa impormasyon sa mga database ng mga manlalakbay – sa partikular, para sa mga dumarating lulan ng mga sasakyang panghimpapawid, tren, o cruise ship – at batay sa mga "pahiwatig" na sa palagay ng Agency ay nagpapalaki sa posibilidad ng isang indibidwal na magkaroon ng ilang kontrabando sa kanyang mga electronic na device. Walang pampublikong listahan ng mga pahiwatig na ginagamit ng Agency, ngunit batay sa mga obserbasyon, mas malaki ang posibilidad na mapili ka para sa pagsisiyasat kung:

- Nag-aangkat ka ng isang bagay na kahina-hinala para sa CBSA, o na nauugnay sa mga kilalang importer o exporter ng mga materyales na tinututulan ng Agency. Maaaring kasama rito ang anime at manga, na lubos na kahina-hinala para sa Agency
- Pumunta ka sa mga "napakamapanganib" na lugar (bagama't walang available na listahan, kasama rito ang mga lugar sa Timog-Silangang Asya, gayundin ang Alemanya, Cuba, at Espanya)
- Mag-isa kang bumibiyahe
- Halatang kinakabahan ka o kung hindi ka mapakali
- Marami kang electronic na device (kasama ang mga hard drive)
- Nagpapakita ka ng interes sa pornograpiya, gaya ng ipinapahiwatig ng mga filename o folder sa iyong device
- Pinakahuling sandali ka na nang bumili ng ticket upang bumiyahe
- May coding sa iyong bagahe na hindi tumutugma sa pinanggalingan mo
- Hindi pangkaraniwan ang iyong mga ruta sa biyahe

Sa paunang pagsisiyasat, hindi masyadong babasahin ng mga opisyal ang bawat dokumento, o hindi nila masyadong susuriin ang bawat larawan sa iyong device. Mabilisan lang nilang titingnan ang mga nabanggit upang matiyak na walang kaugnayan ang mga ito sa kontrabando (gaya ng pornograpiya ng bata), o upang kumpirmahing totoo o hindi totoo ang mga hinala tungkol sa isang paglabag sa batas sa customs o immigration. Maaaring gamitin ang impormasyong makukuha sa isang paunang pagsisiyasat bilang batayan para sa pagsasagawa ng mas masusing pagsusuri.

Ang mismong nilalaman lang ng iyong device ang titingnan ng mga opisyal. Ilalagay nila ang device sa airplane mode, at lokal na nilalaman lang (kabilang dito ang mga email at text message na may markang "nabasa na") ang kanilang titingnan. Hihingi ng warrant ang CBSA sa isang hukom kung malayuan lang naa-access ang impormasyong gusto nilang siyasatin. Gayunpaman, hindi na lingid sa kaalaman ng mga taong hinihiling ng CBSA sa mga manlalakbay na boluntaryong mag-log in sa isang malayuang account, kaya hindi makakaasa ang mga manlalakbay na mananatiling pribado ang kanilang mga naka-link na social media account sa pagtawid nila sa border.

Mga Masusing Pagsisiyasat

Kung makakakita ang isang opisyal ng isang bagay na sa palagay niya ay dapat pa niyang siyasatin, maaaring magsagawa ng mas masusing pagsisiyasat. Ang mga pagsisiyasat na ito ay isinasagawa ng mga espesyalistang eksperto sa mga tool para sa forensics.

Sa masusing pagsisiyasat, kukunin nila ang iyong device. Ang *Customs Act* ay nagbibigay sa CBSA ng kapangyarihang kunin ang mga produkto kung sa palagay ng isang opisyal ay hindi maayos na nasuri ang mga ito para sa pagpasok sa Canada. Maaari ding kopyahin ng mga opisyal ang lahat ng nilalaman ng

iyong device. Dahil dito, magagawa ng CBSA na magpatakbo, sa ibang pagkakataon, ng software na nagka-crack ng password upang ma-access ang anumang bagay na hindi nila natingnan dahil hindi mo ibinigay ang password.

Ayon sa CBSA, hindi na itinatabi ang mga kopya ng datos pagkatapos ng imbestigasyon. Gayunpaman, alam naming maaaring ibahagi at ibinabahagi ng CBSA ang personal na impormasyong nakokolekta nito mula sa mga pagsusuri sa iba pang ahensya ng pamahalaan gaya ng RCMP at iba pang ahensyang panseguridad gaya ng CSIS (na maaari naman nitong ibahagi sa mga pamahalaan sa ibang bansa para sa mga layunin ng pangongolekta at pagsusuri ng impormasyon).

Mga Password

Maaaring hingin ng mga opisyal ang iyong password o fingerprint upang ma-access ang impormasyong nakaimbak sa iyong device. Hindi malinaw kung iniaatas ba ng batas na ibigay mo ito, ngunit may inaresto o binantaan nang arestuhin ang CBSA para sa hindi pagbibigay sa password. Ayon sa CBSA, may karapatan silang mang-aresto ng mga tao para sa hindi pagbibigay ng password, at maaari nila itong gawin kung makatuwiran ang dahilan ng opisyal sa paniniwalang may ipinagbabawal na materyales sa isang device.

Noong 2017, isinaad ng CBSA na hindi nila maaaring puwersahin ang sinumang magbigay ng password upang magkaroon ng access sa anumang account, file, o impormasyon na naka-store nang malayuan. Kung hihingin ang iyong password upang ma-access ang isang online account, hindi ka dapat maharap sa anumang parusa kapag hindi mo ito ibinigay.

Kung hihingin ang iyong password o fingerprint upang ma-access ang impormasyong naka-store sa iyong device at hindi mo ito ibibigay, maaaring mas paghinalaan ng CBSA ang mga nilalaman ng iyong device, hindi ka papasukin kung hindi ka mamamayan o permanenteng residente ng Canada, kunin o kumpiskahin ang device para sa mas masusing inspeksyon ng mga espesyalista sa forensics (na maaaring abutin nang ilang buwan), o arestuhin ka. Ang pagpigil o paghadlang sa isang opisyal ng CBSA ay isang paglabag na maaaring patawan ng multang hanggang $50,000 at/o limang taong pagkakakulong.

Mga Lugar para sa Preclearance ng U.S. sa Canada

Pinapahintulutan ang mga opisyal ng Customs and Border Patrol ng U.S. na ipatupad ang batas ng U.S. sa ilang bahagi ng mga paliparan, istasyon ng tren, at daungan ng ferry sa Canada kung saan maaaring ma-clear sa U.S. customs ang mga manlalakbay papuntang U.S. bago sila umalis sa Canada. Sa mga lugar na ito, napapailalim ang pagpapatupad ng mga batas ng U.S. sa mga batas sa mga karapatang pantao ng Canada, kasama ang *Charter of Rights and Freedoms*. Ibig sabihin, ang mga pamantayan sa pagsisiyasat at pagkumpiska ng Canada ang ginagamit, sa halip na ang mga pamantayan ng U.S. Gayunpaman, hindi malinaw kung may kaalaman o pagsasanay ba ang mga opisyal sa border ng U.S. kaugnay ng mga naaangkop na legal na pamantayan.

Para sa pagsisiyasat ng mga electronic na device, katulad ng mga batas ng U.S. ang mga batas ng Canada: hindi kailangan ng mga opisyal ng warrant o makatuwirang dahilan upang tingnan ang iyong telepono. Lokal na nilalaman lang dapat ito, na hindi nangangailangan ng koneksyon sa network upang makita.

Nagsasagawa ang mga opisyal sa border ng U.S. ng mga karaniwan at advanced na pagsisiyasat. Maaaring magsagawa ng mga karaniwang pagsisiyasat may hinala man o wala, at kasama rito ang anumang pagsisiyasat ng electronic na device, na hindi pa maituturing na advanced na pagsisiyasat.

Sa advanced na pagsisiyasat, ikokonekta ang device sa isang external na kagamitan upang ma-access ang mga nilalaman nito, at kung minsan ay upang makopya rin ang mga ito. Nangangailangan ang mga advanced na pagsisiyasat ng makatuwirang dahilan upang paniwalaang nalalabag ang mga batas ng U.S., o ang isang bagay na nauugnay sa pambansang seguridad.

Maaaring hingin ng mga opisyal sa border ng U.S. ang iyong password. Kung hindi mo ito ibibigay, maaaring tumanggi ang opisyal na i-preclear ka para sa pagpunta sa U.S. Maaari ding kunin ng opisyal ang device para sa isang mas advanced na pagsisiyasat. Hindi dapat manatili sa kanila ang iyong device nang mahigit sa limang araw, ngunit ayon sa mga ulat, kung minsan ay nananatili ang mga device sa kanila nang ilang buwan.

Mga Tip

Sa pag-iisip ng mga pagkilos na gagawin mo upang maprotektahan ang iyong privacy, tandaang maaaring hindi maging maganda ang ugnayan mo sa isang opisyal sa border kung malalaman niyang sinadya mong subukang pigilan ang isang pagsisiyasat, lalo na kung may sinira kang data na maa-access mo naman sana, o kung inilihim mong may ganoon ngang data.

- **Iwan ang iyong mga device sa bahay** kung hindi mo kailangan ang mga ito sa iyong biyahe o **gumamit ng nakalaang device para sa paglalakbay** na walang data o aktibidad.
- **I-backup** ang iyong data bago ka tumawid sa border at iwan ito sa bahay. Mahalaga ito kung sakali mang kunin o kumpiskahin ang iyong device, at magbibigay rin ito sa iyo ng opsyong mag-delete ng hindi kinakailangang data sa iyong device bago ka tumawid sa border. Maaari mo ring alisin ang lahat ng nilalaman ng iyong device bago ka tumawid sa border at i-restore ito mula sa isang backup pagkatapos.
- **Ligtas na i-delete ang data** na hindi mo kailangan sa biyahe. Ibig sabihin, huwag lang ito basta-bastang ilagay sa recycling bin, sa halip, dapat kang gumamit ng mga naka-built in na tool sa Windows (tool na tinatawag na *cipher*), Mac (‘*secure empty trash*’ o *srm*), o Linux (*shred* o *srm*) upang permanenteng mag-delete ng data. Tandaang may access ang mga ahensya sa border sa mga kumplikadong tool sa forensics, at may kakayahan silang makakita ng impormasyon tungkol sa na-delete nang data na hindi kayang gawin ng isang ordinaryong indibidwal. Sa pagpindot ng “delete,” walang garantiyang hindi makikita ng isang opisyal sa border ang nabanggit na impormasyon.
- **Humingi ng password** sa pag-log in o pag-access sa iyong device. Maaaring mawalan na ng interes ang isang opisyal na hindi naman ganoon kagustong mag-usisa, sa oras na i-on niya ang iyong electronic na device upang tingnan ang mga nilalaman nito, kapag nakita niyang kailangan pa niyang hingin ang iyong password.
- **Gumawa ng mahirap hulaang password**, halimbawa, sa pamamagitan ng paggamit ng ilang random na salita (‘passphrase’) kung maaari, at pag-iwas sa mga password na madaling mahulaan.
- **I-off ang iyong computer** bago ka dumaan sa customs, at tiyaking hindi awtomatikong magla-log in ang alinman sa iyong mga account o application kapag na-activate ang mga ito.
- **Gumamit ng two-factor na pag-authenticate**, kung sakali mang makuha ng ahensya sa border ang isa mong device at maiwan sa iyo ang isa.
- **Gumamit ng Full-Disk Encryption** at humingi ng passphrase na mahirap mahulaan upang ma-access ito. Maraming bagong device ang may naka-built in na ganitong opsyon. Mapapanatili nitong ligtas ang iyong data, maging sa pinakamahuhusay na analyst. Gayunpaman, hindi

malinaw kung ano ang mangyayari kapag nakumpiska ang iyong electronic na device at hindi ma-access ng ahensya sa border ang iyong data. Maaaring kumpiskahin at hindi na ibalik ang iyong device.

- Kung ayaw mong gumamit ng Full-Disk Encryption, maaari ka ring **mag-encrypt ng ilang mahahalagang dokumento** o file gamit ang naka-built in na software.
- **Paghiwa-hiwalayin at ilagay ang mga pribado at kumpidensyal na dokumento** sa sari-sariling folder ng mga ito upang malinaw na maipabatid na pribado ang mga ito. Kasama rito ang mga file ng mga abugado, at maaari itong kabilangan, kung minsan, ng mga file ng mga doktor, psychologist at psychiatrist, at mamamahayag. Hindi titingnan ng mga opisyal sa border ang mga pribadong materyales sa oras na ipaalam sa kanilang may mga ganitong materyales, maliban na lang kung kailangan nilang kumpirmahing pribadong materyales nga ang mga ito. Sa pangkalahatan, hindi nila dapat tingnan ang mga pribadong file, ngunit maaaring hindi igalang ng lahat ng opisyal sa border ang batas sa usaping ito.

Paghahain ng Reklamo

Kung sa palagay mo ay hindi naaangkop ang ginawang pagsisiyasat sa iyo, ngunit hindi tungkol sa diskriminasyon o paglabag sa privacy ang iyong reklamo, maaaring sa mismong Canadian Border Services Agency ka maghain ng reklamo. Kung kinumpiska ang iyong device, o kung pinatawan ka ng parusa o multa, maaari mong hilinging suriin ang pasya.

Maaari ka ring magpadala ng nakasulat na feedback sa Recourse Directorate ng CBSA, na maaaring sumuri ng gawi ng mga opisyal. Tiyaking isasama mo ang lahat ng nauugnay na impormasyon upang maunawaan ng recourse officer ang iyong reklamo at magawa niyang makipag-ugnayan sa iyo.

Kung sa palagay mo ay nakaranas ka ng diskriminasyon mula sa isang opisyal ng CBSA, maaari kang maghain ng reklamo sa Canadian Human Rights Commission. Kasama sa mga batayan ng diskriminasyon ang lahi, bansang pinagmulan o etnisidad, kulay, relihiyon, edad, kasarian, sekswal na oryentasyon, kinikilala o ipinapahiwatig na kasarian, marital status, family status, kapansanan, mga genetic na katangian, o isang hatol kung saan nabigyan ng pardon o record suspension ang may sala.

Kung sa tingin mo ay nalabag ng CBSA ang iyong privacy, maaari kang maghain ng reklamo sa Office of the Privacy Commissioner of Canada, na tumitiyak na nakakasunod ang pamahalaan sa Batas ng Pagkapribado.

Maaari mo ring iulat ang anumang nauugnay na insidente sa mga interesadong grupo para sa mga karapatang sibil, kasama ang International Civil Liberties Monitoring Group at/o National Council of Canadian Muslims.

Kung sa palagay mo ay nalabag ang iyong privacy o nakaranas ka ng diskriminasyon mula sa mga opisyal ng U.S. sa mga lugar para sa preclearance, inirerekomenda naming sumulat ka sa Minister of Public Safety at Minister of Foreign Affairs. Maaari ka ring makipag-ugnayan sa Office for Civil Rights and Civil Liberties sa Department of Homeland Security, Chief Privacy Officer ng Department of Homeland Security, at Traveler Redress Inquiry Program ng Department of Homeland Security. Maaari mo ring iulat ang anumang nauugnay na insidente sa mga interesadong grupo para sa mga karapatang sibil, kasama ang Electronic Frontier Foundation, Council on American-Islamic Relations, at American Civil Liberties Union.

www.bccla.org

@bccla

@BCCivLib

www.cippic.ca

@cippic

This project was supported by a grant from the Canadian Internet Registration Authority's (CIRA) Community Investment Program.