ჩვენი დისკუსიის შემდეგ ონლაინში კონფიდენციალურობის შესახებ, გამომდინარეობს რომ ეს მოთხოვნები უნდა დაკმაყოფილდეს ინტერნეტით ინფორმაციის გავრცელებისას.

შემდეგ განვიხილოთ მეხუთე შესწორება, რომელიც გვიცავს ხელისუფლების მოქმედებებისგან, რომელიც შეიძლება გამოწვეული იქნას მასალა საკუთარი თავის დასადანაშაულებლად. შემდეგ დებულებაში ნათქვამია:

„არავინ უნდა იყოს იძულებული ნებისმიერ კრიმინალურ საქმეში რომ იყოს მოწმე თავის წინააღმდეგ.“

ეს არ ეხება იმ შემთხვევას, როცა პიროვნება ნებაყოფლობით აბარებს დოკუმენტებს, ფაილებს, ჩანაწერებს და სხვა ქაღალდებს სამართალდამცავ ორგანოს. ანალოგიურად, კორპორაციის საჯარო დოკუმენტები არ ექვემდებარება ამ დებულებას, მაშინაც კი თუ ისინი შეიცავენ ბრალდებულის საწინააღმდეგო სამხილებს.

აგრეთვე მეხუთე შესწორება შეიძლება საყოველთაოდ იქნას დაკავშირებული სისხლის სამართლის საქმის აღძვრისგან თავის შეკავებაზე, მეხუთე შესწორება აგერეთვე მოიპოვება ონლაინ აპლიკაციის სახით მსოფლიოს მასშტაბით. მეხუთე შესწორების საინტერესო პროგრამა კიბერუსაფრთხოებაზე მოიცავს მოქმედებებეს დასაშიფრ(დაშიფრულ) ფალზე რომელიც შეიძავს შესაძლო მამხილებელ ინფორმაციას.

დაშიფრრა შეიცავს დაშივფრის მეთოდებს რომ დაიბლოკოს წვდომა კონკრეტულ დოკუმენტებზე. „Doe v. United States”-ში, უზენაესმა სასამართლომ დადგინა ინდივიდს შესაძლოა დაეკისროს „გახდეს იძულებული რომ თქვას გასაღები მამხილებელი დოკუმენტის, მაგრამ არა თავისი კედლის სეიფის“

ეს შემთხვევა როგორც ჩანს, გულისხმობს, რომ სამართალდამცავ ორგანოებს მართებული ძიების შედეგად შეუძლიათ მიიღონ დაშიფრული ფაილი. თუმცა Doe-ს გადაწყვეტილება ხელს შეუშლის სააგენტოს რომ მოპასუხეს მიაწოდოს პაროლი , გასაღები ან კოდი რომელიც დეშიფრავიის ან დეკოდირების საშუალებას მისცემს. Doe სვამს კითხვებს თანამშრომლებთან დაკავშირებით, რომლებიც ინახავს პოტენციურად კრიმინალურ ინფორმაციას მათი დამსაქმებლის კომპიუტერებზე. თუ ინფორმაცია ეკუთვნის დამსაქმებელს და არა თანამშრომელს (ანუ დასაქმებულს), შესაძლებელია რომ სასამართლომ დაუშვას ეს გახდეს მისთვის ხელმისაწვდომი და გამოიყენოს ის არა მართო დასაქმებულის განთავისუფლებისთვის არამედ ნებისმიერი სამართალდამცავი ქმედების შემთხვევაში. რასაკვირველია ეს გულისხმობს, რომ კომპანიას აქვს უნარი რომ მოითხოვოს დასაქმებულზე წვდომა, როგორც კომპანიის პოლიტიკის ან მოქმედი კანონის სახელით.

**სახელმწიფო კონსტიტუცია**

დამატებით ამერიკის კონსტიტუციის გარდა, სახელმწიფო კონსტიტუცია კონფიდენციალურობის უფლების წყაროა. ზოგადად, სახელმწიფო კონსტიტუცით დადგენილი კანონები ანარეკლია შესწორებების, რომლებიც განვიხილეთ წინა თავში და, შესაბამისად მხოლოდ საჯარო მოხელეების მიმართ. თუმცა ზოგიერთი სახელმწიფო მეტ კონფიდენციალურობას ანიჭებს სახელმწიფოს კონდიდენციალურობის დარღვევებს. კონსტიტუციური დაცვის მიღმა, სახელმწიფოები მნიშვნელოვან როლს ასრულებენ კონფიდენციალურობის რეგულაციებში, მრავალრიცხოვანი კანონებით, რომლებიც ითვალისწინებენ კონფიდენციალურობის დაცვას და მონაცემთა უსაფრთხოების მოთხოვნებს. ამგვარი ზომები განიხილება

**საერთო სამართლის კანონები კონფიდენციალურობის შემოჭრისას**

საერთო სამართლის და კანონთა კრებულის მიხედვით აღიარებულია ოთხი ძირითადი კონფიდენციალურობის კანონი. ეს წესები უზრუნველყოფენ ფულადი სახრებისა და სასამართლო აკრძალვის შესახებ არაკონსტუტიციურად ან არასანქციებულად შეჭრის კონფიდენციალურობის უფლებებს. მათ ასევე შეუძ₾იათ უზრუნველყონ სამათლებლივი დაცვის საშუალებები, რომლებიც დაკავშირებულია კონფიდენციალურობის უფლებასთან პირდაპირ. ეს ოთხი კანონია : (1)შეჭრის შეწყვეტა (2) კერძო ფაქტების საჯარო გამჟღავნება, რამაც ზიანი მიაყენა რეპუტაციას (3)საჯაროდ ცილისწამება და (4)პიროვნების სახელის ან მსგავსების მითვისება, რამაც ზიანი მიაყენა მის რეპუტაციას, თითოეული მათგანი განხილულია ქვემოთ:

**შესვლის აკრძალვა**

თითოეული ჩვენგანის უფლებაა შეგვეძლოს გარკვეულ ადგილას წასვლა განმარტოებით და მარტო დარჩენა მაგრამ ეს არ არის სრულყოფილი. თუმცა როდესაც სხვა პიროვნება ნებართვის ან სამართლებლივი დასაბუთების გარეშე არღვევს ადგილსამყოფელის ადგილს, რომ ინდივიდი შეიძლება აღმოჩენილიყო ამ სამართალდარღვევის ჩამდენი. სამართალდარღვევის კოდესს განსაზღვრავენ შეჭრას განმარტოებით როგორც :

განზრახ შეჭრა, ფსიქიკურად ან სხვაგვარად, სხვის მარტოობის(solitude) ან მისი პირადი საქმეების ან შეშფოთების საფუძველზე.

იმისათვის რო გაგრძელდეს პროცესი, მოსარჩელემ უნდა დაამტკიცოს შემდეგი ელემენტები:

1. იყო განზრახ შემოჭრა, ან იცოდა რომ ეს შემოჭრა არასწორი იქნებოდა
2. ოყო სავარაუდო მოლოდინი კონფიდენციალურობის დარღვევის
3. შემოჭრა იყო რეალურად შეურაცმყოფელი ადამიანისთვის.

**STEINBACH V. VILLAGE OF FOREST PARK**

სტეინბახს, ადგილობრივი არჩეული თანამდებობის პირს, მუნიციპალიტეტის მიერ გაცემული ელ-ფოსტის ანგარიში აქვს. მესამე მხარის კომპანია, ჰოსტვეი, რომელმაც უზრუნველყო ანგარიშის ტექნოლოგია. სტეინბახი შედის ჰოსტვეის, ვებ-გვერდის ანგარიშზე და ამჩნევს შეტყობინებებიდან თერთმეტი შეტყობინება გაგზავნილი იყო სხვის მიერ საწინააღმდეგო პოლიტიკურ გუნდთან. სეინბახმა უჩივლა მუნიციპალიტეტს, მისი პოლიტიკური მეტოქის და აიტი მიმართულების თანამშრობლების გამო რომლებიც დანიშნული იყვნენ მუნიციპალიტეტის ხელშეწყობით. მაინ შეიძინა რამდენიმე პრეტენზია მათ შორის ფედერალური მოსმენის აქტი, შენახული კომუნიკაციების აკქტი და კომპიუტერული თაღლითობის და ბოროტად გამოყენების აქტი. მან ასევე შეიტანა სარჩელი ილინოისის საერთო სასამართლოში შეჭრის შეწყვეტის შესახებ.

**სასამართლოს მოსაზრება**

მომჩვანმა ამ საქმეში მიიტანა რიგი პრეტენზიები. ყველაზე რელევანტური არის სასამართლოს განხილვა იმის შესახებ რომ შეჭრა მოხდა უნებართვოთ და მიიჩნევა სამართალდარღვევად. მართალია, რომ ილინოისის უზენაესმა სასამართლომ არ აღიარა შეჭრის ფაქტი, სასამართლომ დაადგინა რომ სამართალდარღვევა არ არსებობდა. როდესაც სახელმწიფო სადავო სამარტალი გაურკვეველია, ფედერალურმა რაიონულმა სასამართლომ დაადგინა გეოგრაფიული არეალი, სადაც სავარაუდო დანაშაული მოხდა, თუ არ არის იმის საფუძველი, რომ უზენაესმა სასამართლომ სხვაგვარად გადაწყვიტოს. სახესხვაობების საქმეში არის ის თუ რა უნდა გააკეთოს სახელმწიფოს უმაღლესმა სასამართლომ, რომელიც შეიძლება ჩავთვალოთ მთავარ კითხვად. ტყის პარკი მდებარეობს მზარეულის ქვეყანაში(Cook country), რომელიც პირველ რაიონშია, პირველი ინსპექციის სააპელაციო სასამართლოდან იმართება.პირველმა რაიონმა ოფიციალურად აღიარა ილინოისში დანაშაულის არსებობა. აქედან გამომდინარე, ეს სასამართლო აღიარებს პირველი საოლქო სასამართლოს გადაწყვეტილების არსებობას, ვინაიდან ილინოისის უმაღლეს სასამართლოში არ არსებობს სადავო არგუმენტი. Busse- ის ფარგლებში, კანონდარღვევის ოთხივე ელემენტი უნდა დაკმაყოფილდეს. ეს ელემენტებია : (1) მოპასუხემ ჩაიდინა არასათანადო დანაწილება მოსარჩელის შეწყვეტის შესახებ; (2) შეჭრა იქნება ძალიან დამამცირებელი reasonable პირისათვის; (3) ეს საკითხი იყო კერძო; და (4) ჩარევამ გამოიწვია მოსარჩელის დაზიანება.

კალდერონი ამტკიცებს რომ მისი წვდომა სტეინბახის მეილზე იყო ავტორიზებული ილინოისის შტატის მიერ. 3.1-35-20 ნაწილის თანახმად, "მერს ან პრეზიდენტს ნებისმიერ დროს შეუძლია შეისწავლოს და შეამოწმოს მუნიციპალიტეტის ნებისმიერი აგენტის, თანამშრომლის ან ოფიცრის წიგნები, ჩანაწერები და დოკუმენტები. მართალია, "ჩანაწერები" მოიცავს ყველფერს "ციფრული ელექტრონული მასალის", მათ შორის ელ-ფოსტას განსაზღვრების ჩათვლით. ხოლო მინიმალური საქმის სამართალის დებულების განმარტებისას ნათელია, რომ არ აძლევს მერ კარტ ბლანკს უფლებას, გამოიყენოს ჩანაწერები საკუთარი მიზნებისთვის. ერთ შემთხვევაში, სასამართლომ დაადგინა, რომ ქალაქის მერს უფლებამოსილი ჰქონდა წვდომა ქონოდა პირადი არასრულწლოვანის ჩანაწერებე, რომელიც ეჭვქვეშ აყენებდა პოლიციელის ქცევას. ეს წვდომა განსხვავდება იმისგან, რაც ბრალად წაეყენა კალდერონს. ურბანაში მერმა არ გამოიყენა პირადი სარგებლობის წვდომის უფლება, თუმცა ოფიციალური ქალაქის გამოძიება დაკავშირებულია მერის თანამდებობაზე. კალდერონმა არ გამოიყენა სტეინბახის- ის ელ-ფოსტა ნებისმიერი ოფიციალური მიზნისთვის, არამედ საკუთარი პირადი მოგებისთვის. აქედან გამომდინარე, განსასჯელმა განაცხადა, რომ მისი ქმედებები კანონიერად უფლებამოსილი იყო. კალდერონი ასევე ამტკიცებს, რომ სტეინბახმა არ იცის სათვალთვალო წერილების კონფიდენციალურობა. დამოწმებული მესამე შეცვლილი საჩივრით, სტეინაბახი ირწმუნება, რომ წერილები განკუთვნილი იყო პირადი მოხმარებისთვის. სტეინბახი საკმარისად აღიარებს სამოქალაქო კანონდარღვევის მესამე ელემენტს to survive Motion to Dismiss. იმის განსაზღვრა ელ-ფოსტა იყო თუ არა რეალური არის შეკითხვა და რომლის განსაზღვრაც ამ ეტაპზე შეუძლებელია. ამიტომ მე-8 მუხლი უნდა დადგეს.

**საქმის შეკითხვები**

1. რა ელემენტებია სამართალდარღვევის შეჭრის ფაქტები?
2. **ეთიკური მოსაზრება:** თქვენ ფიქრობთ, რომ არსებობს უკანონოდ შემოჭრის როლი, რომელიც ირღვევა ონლაინ სამყაროში თუ ის უფრო შეზღუდულია რეალურ სამყაროში.
3. ხოლო მოსარჩელეებმა წარმატებით მოიპოვეს ინტერნეტ-საქმიანობისთვის შეჭრის სამართალდარღვევის წინააღმდეგ პრეტენზია, სხვა მოსარჩელეებმა მსგავსი წარმატება არ ისურვეს. რა არის კონკრეტული შეფერხებები იმ ბრალდებების შეტანაზე, რომლებიც ხელს უშლის კონფიდენციალურობის დარღვევას ინტერნეტში?

**კერძო ფაქტების საჯაროდ გამჟღავნება, რამაც ზიანი მიაყენა რეპუტაციას**

რეპუტაციაზე ზიანის გამომწვევი კერძო ფაქტის საჯაროდ გამჟღავნება ეხება საზოგადოებრივ გამჟღავნებას ან გადაცემას მაღალ პირად ფაქტორებს ან ინფორმაციას იმ პირზე, რომელიც რეპუტაციის დაზიანებას იწვევს.ზოგიერთ შემთხვევაში, სამართალდარღვევა უკავშირდება დისკრეტიტაციას და ორივე შეიძლება გამოვიყენოთ როგორც ცალკეული მიზეზები იმავე საქმეში.

დამატებით "განზრახვა და ცოდნა" და "გონივრული პირისადმი მაღალი შეურაცხყოფა" -ს ელემენტები, კერძო ფაქტორების საჯაროდ გამჟღავნება იწვევს რეპუტაციის დაზიანებას და მოითხოვს: 1. ფაქტები უნდა იყოს კერძო; და 2. კომუნიკაციიები თუ რეკლამები უნდა იყოს საზოგადოების მნიშვნელოვანი სეგმენტის განსახილველი. უფრო მეტიც, ეს დანაშაული ჩადენილია, როდესაც ფაქტების გამოქვეყნება იქნებოდა (1)შეურაცმყოფელი კონკრეტული პიროვნებისთვის და (2)არ არის კანონიერი საზოგადოდ განცხადებისთვის.

**საჯაროდ დებს სხვას ბრალს (ცილისწამება)**

სამართალდარღვევის კოდექსის მიხედვით:

ვინც საჯაროდ მიმართავს სხვა საკითხს, რომელიც საზოგადოებას აყენებს სიცრუეში, პასუხისმგებელია მეორე მხარის კონფიდენციალურობის შელახვისთვის თუ

(ა) სიცრუე რომელიც განაცხადა მეორე პირმა, ზიანს აყენებს პიროვნებას და

მოქმედმა პირმა იცოდა, რომ მოქმედებდა უგუნურად, და იწვევდა პიროვნების საჯაროდ შელახვას და შეყავდა შეცდომაში.

ცრუ ხედვის საჯაროდ განთავსება ასევე უკავშირდება ცილისწამებას და მოიცავს ცრუ პიროვნებას, რომელიც დაკავშირებულია ამორალური, უკანონო ან უხერხულ მდგომარეობასთან, რის შედეგადაც ხდება ადამიანის რეპუტაცის შელახვა. დღეისათვის ეს პროცესი არ ყოფილა ბევრის საგანი, სამართალწარმოება უკავშირდება ონლაინ საქმიანობას.

**პიროვნების სახელის მითვისება ან მიმსგავსება რომელიც ზიანს აყენებს პიროვნების რეპუტაციას**

პიროვნების სახელის ან ზედმეტსახელის მითვისება, რომელიც ზიანს აყენებს მის რეპუტაციას, ჩვეულებრივ მოიცავს ცოცხალ პიროვნების სახელის გამოყენებას ან კომერციული და არაკონკურენტული მიზნისთვის ნებართვის გარეშე. არსებობს სამი ელემენტი, რომელიც უნდა იყოს ნაჩვენები, რომ დაამტიცო ამ დანაშაულის სინამდვილე: (1)პიროვნების სახელი, პორტრეტი ან სურათი გამოიყენეს (2)ვაჭრობის ან რეკლამის მიზნით; (3)პიროვნების წერილობითი თანხმობის გარეშე.

მაგალითი სასჯელაღრულების კოდექსიდან არის შემდეგი: „ა არის მოქმედი პირი, ცნობილი თავისი ლამაზი ფიგურით, ბ-ს სურს გაუკეთოს თავის რეკლამა პურს, და აკეთებს განცხადებას გაზეთში რომელსაც ერთივს ა-ს სურათი და სათაურად აქვს „შეინარჩუნე ასეთი ფიგურა ბ-ს rye and whole wheat პურის მეშვეობით. ამ შემთხვევაში ბ-მ დაარღვია ა-ს კონფიდენციალურობა.

**ფედერალური კონფიდენციალურობის კანონი**

სხვა ქვეყნებთან შედარებით, მათ შორის ევროპულ კავშირის წევრ ქვეყნების ჩათვლით, შეერთებულმა შტატებმა მიიღო მონაცემთა კონფიდენციალურობის საკმაოდ მწირი დამოკიდებულება. იმის ნაცვლად, რომ ყოფილიყო ერთი ყოვლისმომცველი მონაცემთა კონფიდენციალობის კანონი, რომელიც გავრცელდებოდა მთელს ინდუსტრიაზე, ამერიკული კანონმდებლები განსაკუთრებულ დაცვას ანიჭებენ გარკვეულ ტიპებს, როგორიცაა სამომხმარებლო კრედიტების ინფორმაცია, სამედიცინო ჩანაწერები და ვიდეო გაქირავების მონაცემებიც კი.

ხოლო ამერიკელი კანონმდებლები ჯერ ვერ არჩევენ კონფიდენციალურობის კანონმდებლობას, რომელიც შეეხება ყველა სახის პერსონალურ მონაცემს. მიუხედავად იმისა, რომ ამ კანონებს შეზღუდული ფარგლები აქვთ, ისინი ზოგადად ქმნიან ფართო მოთხოვნებს და მკაცრ შეზღუდვებს, რომლებიც ეხება კონკრეტული ტიპის პირადი მონაცემების შეგროვებას და გამოყენებას.

**კონფიდენციალურობის დაცვის აქტი**

კონგრესმა აამოქმედა კონფიდენციალურობის დაცვის აქტი, რათა შეამცირონ სამართალდამცავთა ჩხრეკისა და ყადაღის დადების ფაქტები. კონფიდენციალურობის დაცვის აქტი უკრძალავს სახელმწიფო მოხელეებს, რომლებიც ცდილობენ საზოგადოებრივი აზრის გაზიარების მიზნით საზოგადოებრივ მოღვაწეობასთან დაკავშირებული ნებისმიერი სამუშაო პროდუქტის ან დოკუმენტური მასალების მოძიებას ან ჩამორთმევას, თუ საზოგადოებასთან კომუნიკაციის სხვა ფორმით, არსებობს სავარაუდო მიზეზი იმისა, რომ გამომცემელმა შეასრულა ან ჩაიდენს სისხლის სამართლის დანაშაულს, რომელსაც მასთან დაკავშირებული მასალები უკავშირდება. კონფიდენციალურობის დაცვის აქტი ეფექტურად ძალუძს სამართალდამცავ ორგანოებს გამოიყენოს სასამართლო უწყისები ან ნებაყოფლობითი თანამშრომლობა, რათა მიიღონ მტკიცებულება იმ პირთაგან, რომლებიც მონაწილეობენ პირველი ცვლილებების განხორციელებაში.

**1974 წლის კონფიდენციალურობის აქტი**

1974 წლის კონფიდენციალურობის აქტი მოიცავს თითქმის ყველა პირად ჩანაწერს, რომელსაც ახორციელებს ფედერალური სააგენტოები და ზოგიერთი ფედერალური კონტრაქტორები. ეს ეხება სამხედრო სამედიცინო ჩანაწერებს, ვეტერანთა ჩანაწერებს, ინდოეთის ჯანდაცვის სამსახურებს, მედიკამენტების ჩანაწერებს და სხვა ფედერალური სააგენტოების სამედიცინო ჩანაწერებს. 1974 წლის კონფიდენციალური აქტი არ ვრცელდება საავადმყოფოების, კლინიკების ან ექიმების მიმართ, მაშინაც კი, თუ ისინი იღებენ ფედერალურ ფონდებს ან საგადასახადო თავისუფლდება. ზოგადად, 1974 წლის კონფიდენციალური აქტის თანახმად, ადამიანებს ოთხი უფლება ანიჭებს: (1) მოიძიონ ინფორმაცია, თუ რა ინფორმაციას აწვდიდა მათ მთავრობა; (2) რომ ნახონ, და ქონდეთ, ინფორმაციის ასლი , (3) შეცვალონ ან შეასწორონ ან ეს ინფორმაცია; და (4) გამოიყენოს შეზღუდული კონტროლი ამ ინფორმაციის გამჟღავნებაზე სხვა მხარეთათვის.

**საკაბელო საკომუნიკაციო პოლიტიკის აქტი**

საკაბელო საკომუნიკაციო პოლიტიკის აქტი ამოქმედდა 1943 წლის კომუნიკაციების აქტის შესწორების მიზნით. საკაბელო აქტი აწესებს საკაბელო რეგულირების ყოვლისმომცველ ჩარჩოს და აბონენტის კონფიდენციალობის ძლიერი დაცვის პირობებს ადგენს აბონენტის მონაცემების შეგროვების, შენარჩუნებისა და გავრცელების შეზღუდვის გზით.იგი კრძალავს საკაბელო სისტემების ოპერაციებს საკაბელო სისტემის გამოყენებით , რომლითაც შეუძლება შეგროვდეს "პირადად იდენტიფიცირებული ინფორმაცია" შეგროვება ნებისმიერი აბონენტის შესახებ წინასწარ თანხმობის გარეშე, თუ ინფორმაცია არ არის საჭირო მომსახურების გაწევისთვის ან არაავტორიზებული მიღების გამოვლინებისთვის. იგი ასევე კრძალავს ოპერატორებს მესამე პირისთვის პირადობის იდენტიფიცირების მონაცემების თანხმობის გარეშე გადაცემას, თუ არ არის აუცილებელი გამჟღავნება საკაბელო ოპერატორის მიერ გაწეული მომსახურების გაწევისათვის ან იმ შემთხვევაში, თუ იგი გადაეცემა სასამართლოს სახელმწიფო ბრძანებით.

**ვიდეო კონფიდენციალურობის დაცვის აქტი**

ვიდეო კონფიდენციალურობის დაცვის აქტის მიზანია მომხმარებელთა ვიდეო გაქირავების ისტორიების კონფიდენციალურობის დაცვა. შეზღუდული გამონაკლისების გათვალისწინებით, აქტი კრძალავს ვიდეოკონტექსტის მომსახურების მიმწოდებლებისთვის პირადობის იდენტიფიცირების შესახებ ინფორმაციის გამჟღავნებისგან, რომლებიც მესამე პირებს ქირაობენ ან ყიდულობენ. აქტი ითვალისწინებს, რომ მომხმარებელს შეუძლია მოქმედება მოახდინოს ნებისმიერი ვიდეო მაღაზიის წინააღმდეგ, რომელიც გამოაქვს პირადი საიდენტიფიკაციო ინფორმაცია. ფაქტობრივი ზიანის ამოღება ხდება აქტით, მაგრამ ლიკვიდირებული ზიანის ოდენობა არ უნდა იყოს ნაკლები $ 2 500. გარდა ამისა, სადამსჯელო ზიანი, ისევე როგორც ადვოკატის საფასური,სადაზღვევო ხარჯები და "წინასწარი და თანასწორი" დახმარება შეიძლება იყოს აღდგენადი საჭიროების შემთხვევაში. აქედან გამომდინარეობს სამართალწარმოების შეზღუდვის ორწლიანი დებულება.

**სატელეფონო სამომხმარებლო დაცვის აქტი**

1991 წლის სატელეკომუნიკაციო დაცვის აქტი მოქმედებდა სამომხმარებლო საჩივრების საპასუხოდ ინტრუზიული ტელემარკეტინგის პრაქტიკის და შეშფოთების შესახებ მომხმარებელთა კონფიდენციალურობის შესახებ. 1991 წლის სატელეკომუნიკაციო დაცვის აქტი მოქმედებდა სამომხმარებლო საჩივრების საპასუხოდ ინტრუზიული ტელემარკეტინგის პრაქტიკის და რაც შეეხება მომხმარებელთა კონფიდენციალურობაზე ზიანის მიყენებას. აქტი მოქმედებს 1934 წლის კავშირგაბმულობის აქტის II ნაწილის სახით და მოითხოვს ფედერალური კომუნიკაციის კომისიას "საცხოვრებელი სახლის აბონენტთა უფლებების დაცვის მიზნით" წესების გამოქვეყნებას.TCPA- ს საპასუხოდ, FCC- მა გამოსცა ანგარიში და შეკვეთა, რომელიც ითხოვს ტელემარკეტინგში ჩართულ ნებისმიერ პირს ან მომხმარებელს, რომ შეინარჩუნოს მომხმარებელთა სია, რომლებიც მოითხოვენ რომ არ გამოიძახონ.

TCPA კიდევ უფრო ზღუდავს ავტომატური დარეკვის სისტემების გამოყენებას, ხელოვნური ან წინასწარ შეტყობინებების შეტყობინებებს, მობილურ ტელეფონებზე გამოგზავნილ SMS ტექსტურ შეტყობინებებს და არასასურველი რეკლამის გასაგზავნად ფაქსის აპარატების გამოყენებას. იგი ასევე ზღუდავს ადვოკატებს 8a.m -დან 9 p.m-მდე დარეკვისგან.ფიზიკურ პირებს უფლება აქვთ მოახდინონ ზიანის ანაზღაურება პირდაპირ ადვოკატისგან 500-დან $ 1500-მდე, თითოეული დარღვევისთვის ან რეალური ფულადი ზარალის აღდგენა, რომელიც უფრო მაღალია.

**ელექტრონული კომუნიკაციის კონფიდენციალურობის აქტი(ECPA)**

ელექტრონული კომუნიკაციების კონფიდენციალურობის შესახებ კანონმდებლობა აწესებს აკრძალვებს ელექტრონული კომუნიკაციების აღკვეთის შეზღუდვაზე და ქმნის ელექტრონული კომუნიკაციების კონფიდენციალურობის დაცვას. ECPA აშენდა წარსულში კანონით და ამოქმედდა ელექტრონული დაკვირვების სფეროში პოტენციური დარღვევებისა და კონსტიტუციური დარღვევების წინააღმდეგ