PODSTAWY PRAWA WŁASNOŚCI INTELEKTUALNEJ

Ta część nie jest przeznaczona dla prawników i studentów prawa. Jest raczej napisana dla profesjonalistów komputerowych, którzy mogą uznać za użyteczne zrozumienie, w jaki sposób ich obawy w pracy pasują do ram prawnych, oraz w jaki sposób te ramy kształtują strategie, które mogą wykorzystać w swojej pracy. Nie ma być definitywny, ale pomóc czytelnikom dostrzec problemy, gdy się pojawią, i przekazać zrozumienie, które jest pierwszą częścią w pełni zintegrowanego programu bezpieczeństwa komputerowego. Cyberlaw to kompendium tradycyjnego prawa, które zostało zaktualizowane i zastosowane do nowych technologii. Gdy powstały luki lub tradycyjne prawo jest niewystarczające, uchwalono określone ustawy. To trochę jak stara historia trzech niewidomych i słonia: Jeden z niewidomych dotykających nogi słonia wierzy, że dotyka drzewa; drugi, dotykając jego ucha, wierzy, że jest skrzydłem, a trzeci, dotykając ogona, uważa go za węża. Kwestie cyberprzestrzeni, danych elektronicznych, sieci, transmisji globalnych i pozycjonowania nie mają ani prostych rozwiązań jednostkowych, ani prostego prawa do konsultacji. Myśląc o stosowaniu prawa do bezpieczeństwa komputerów, warto pomyśleć o problemach jako problemach, w których znajduje się komputer

*Cel działania

* Narzędzie używane do działania

* Przypisuje się do samej działalności

Na przykład „włamanie" do komputera może być analogiczne do czynu niedozwoloneg (tj. wpisanie własności innej osoby bez zezwolenia), a „łamanie" może być postrzegane jako konwersja cudzej własności. Podobnie korzystanie z komputera w celu wykonywania nielegalnych kopii stanowi naruszenie praw autorskich w najbardziej podstawowym znaczeniu. Chociaż znak towarowy ma bardzo niewiele wspólnego z komputerami, używanie nazw handlowych jako części słów kluczowych dla wyszukiwarek lub nazw domen w celu przekierowania ruchu internetowego do konkurencyjnej witryny internetowej może stanowić naruszenie znaku towarowego. Dotykając niektórych bardziej tradycyjnych środków zaradczych, ta częśćł skupia się na prawach własności, które są naruszane przez takie działania oraz na środkach zaradczych, które istnieją w kontekście działalności gospodarczej. Uznając, że przepisy prawne dotyczące tych problemów są tak globalne, jak sam Internet, ta część ma pomóc czytelnikom w zobaczeniu słonia w pokoju. Wybierając kwestie prawne, które należy podkreślić, staraliśmy się rozważyć rutynowe potrzeby profesjonalisty komputerowego. Skupiliśmy się głównie na prawie USA, uznając, że te problemy i tematy często przekraczają granice państw. Jest ku temu bardzo prosty powód. Najczęściej wpływ ataku bezpieczeństwa komputera, odmowa usługi, deszyfrowanie lub kradzież materiałów komputerowych pojawią się tutaj lub będą miały bezpośredni wpływ, bez względu na to, skąd pochodzi. Wyobraź sobie przez chwilę bandytę - stojącego w Kanadzie - który celuje w kogoś w Stanach Zjednoczonych, pociąga za spust i uderza w cel. Ponieważ istnieje celowe postępowanie wymierzone w ten kraj, w zwykłym przypadku sądownictwo USA nie tylko zapewni jurysdykcję nad rewolwerowcem, ale także stosować jego prawa. Mogą istnieć inne problemy, takie jak faktyczne złapanie bandyty, ale przykład podkreśla znaczenie prawa Stanów Zjednoczonych dla podmiotów znajdujących się tutaj. Dla celów orientacyjnych zamieściliśmy również sekcję na końcu tego rozdziału, która omawia niektóre problemy międzynarodowe. Jeszcze jedna uwaga wprowadzająca: Używamy wyrażenia „program bezpieczeństwa" w tej części z pewną częstotliwością. Zrozumienie, że to wyrażenie może oznaczać dla prawnika lub menedżera ryzyka coś innego, a innego dla profesjonalisty ds. bezpieczeństwa komputerowego, zamierzamy, aby było to skrótowe odniesienie do ogólnych i systemowych wysiłków w celu zabezpieczenia informacji przechowywanych na komputerach, a nie tylko do aplikacji, które mogą być zatrudnionym jako część tego wysiłku.

NAJBARDZIEJ PODSTAWOWE NARZĘDZIE BIZNESOWE OCHRONY TECHNOLOGII TO UMOWA

Zadaniem specjalisty ds. bezpieczeństwa komputerowego jest zrozumienie, przewidywanie, a następnie martwienie się o ryzyko: ryzyko, które jest poza kontrolą i ryzyko, które można kontrolować. Najbardziej podstawowym narzędziem kontroli ryzyka, przewidywalnym lub nieprzewidywalnym, jest umowa. W przeciwieństwie do innych form kontroli ryzyka, umowa nie musi być statyczna; może być adaptowalny. Możemy ograniczyć użycie; możemy ograniczyć dystrybucję; możemy narzucić warunki i poufność; możemy określić prawa, a także przewidzieć pewne środki zaradcze w drodze umowy. Umowy rzeczywiście mogą przybierać różne formy: tradycyjna podpisana umowa; wymiana wiadomości e-mail, strona internetowa lub warunki użytkowania produktu; umowy o pracę; podręczniki i polityki dotyczące miejsca pracy; i tak zwane umowy typu shrinkwrap lub click-wrap. Sprzedajemy lub licencjonujemy produkty. Gdzie możemy zawrzeć umowę, możemy również zdefiniować i ograniczyć ryzyko.

ZAPOBIEGANIE ROZPOCZYNA SIĘ W DOMU- OBOWIĄZKI PRACOWNIKA I POWIERNIKA

W prawie istnieje stara koncepcja oszustwa, zgodnie z którą pracownicy są winni swoim pracodawcom powierniczy obowiązek najwyższej lojalności. Zakres i zakres tego obowiązku powierniczego jest kwestią prawa zwyczajowego, która różni się w każdym państwie. Ogólnie rzecz biorąc, obowiązek powierniczy pracowników zabrania im korzystania z jakiejkolwiek nieruchomości należącej do pracodawcy w konkurencji z pracodawcy lub osobistych korzyści. Pracownicy mają jednak prawo do zatrzymywania i wykorzystywania, bez względu na cel, własnych umiejętności i wiedzy, co może obejmować kontakty, które rozwijają się w trakcie zatrudnienia, chyba że są to tajemnice handlowe. To, co wchodzi lub nie wchodzi w zakres obowiązku powierniczego, zrodziło niekończące się argumenty i procesy sądowe. Istnieje prosty środek zaradczy na ten problem: umowa, która obejmuje kwestie technologiczne i własność, a także obejmuje wynagrodzenie i inne korzyści.

UMOWA O PRACĘ, PRACĘ, PODRĘCZNIK I PODRĘCZNIK ORGANIZACJI.

Niezależnie od polityki , specjalista ds. bezpieczeństwa powinien zostać wdrożony poprzez umowę o pracę, podręcznik i podręcznik organizacji. Można zastosować wiele postanowień umownych, takich jak: umowy o nieujawnianiu; definicja polityki własnościowej; restrykcyjne przymierza; ustępstwa własności dotyczące odkryć, know-how, ulepszeń, wynalazków itp. w okresie zatrudnienia; zasady dotyczące poczty elektronicznej; warunki użytkowania dotyczące systemów komputerowych; oraz oświadczenia o autoryzowanej i nieautoryzowanej działalności. Chodzi o to, że umowy o pracę i podręczniki powinny stanowić punkt wyjścia dla bezpieczeństwa komputerowego.

PRAWO DO TECHNOLOGI I DOSTĘ W UMWACH ZE SPRZEDAWCAMI I UŻYTKOWNIKAMI

Ochrona bezpieczeństwa musi koniecznie obejmować czujność na wszystkie umowy i licencje ze sprzedawcami i użytkownikami. To może nie być seksowne, ale blokuje i walczy. Dostawcy mogą podlegać wielu takim samym ograniczeniom i umowom o nieujawnianiu, jak pracownicy. Prawa dostępu do sieci intranet i danych powinny być kontrolowane i określone uprawnienia. Należy starannie rozważyć, jakie prawa będzie posiadał użytkownik, zasady dotyczące dostępu użytkownika i egzekwowania tych zasad. Czy to sprzedaż czy licencja? Istnieje wiele zalet kontrolowania technologii poprzez licencje (w przeciwieństwie do sprzedaży), w tym nakładanie limitów na prawa użytkowania i określanie środków zaradczych w przypadku naruszenia licencji lub nieautoryzowanej działalności, która obejmuje licencjonowany produkt. Licencje typu „shrink-wrap” lub „click-wrap” stały się popularnym językiem. Obecnie są one akceptowanymi narzędziami do licencjonowania i kontrolowania dystrybucji oprogramowania tak długo, jak: (a) są biznesem dla biznesu, a zatem między stronami o mniej więcej równej pozycji przetargowej; (b) ich warunki dla innych użytkowników lub

konsumentów nie są nieuzasadnione; oraz (c) nie naruszają porządku publicznego. Pojawiają się obawy co do tego, czy warunki umowne są nieuzasadnione lub umowy wiążą się z przynależnością, ponieważ licencje nie są produktami negocjacji, lecz pełnomocnictwami, które użytkownicy akceptują, gdy otwierają opakowany pakiet lub klikają online. Obawy te zostały rozwiązane dzięki wymogom, zgodnie z którymi użytkownicy otrzymali odpowiednie powiadomienie o warunkach, możliwość odrzucenia i zachowanie, które wystarczająco wyraża zgodę. W przypadku umów na kurczenie się towarów otwarcie produktu, jego instalację i zatrzymanie uznano za wystarczające do wykazania zgody na warunki licencji, zauważając, że jeśli konsument nie wyrazi zgody, produkt może zostać zwrócony. Tak więc potencjalny użytkownik nie musi znać wszystkich warunków licencji przed zakupem, jeśli środek zaradczy obejmuje zwrot po zakupie. Licencja może nakładać ograniczenia użytkowania, ograniczyć liczbę komputerów, na których można zainstalować produkt, kopiować, a nawet dostępne środki zaradcze. Kwestie wypowiedzenia, rzeczywiste lub konstruktywne, możliwość zaakceptowania lub odrzucenia oraz okazanie zgody doprowadziły do ogólnej akceptacji umów online, takich jak prezentacja warunków licencyjnych, po których następuje aktywna potrzeba sprawdzenia, zaakceptowania lub odrzucenia przez kliknięcie odpowiednie pole. Ta sama analiza dotyczy warunków użytkowania, zwłaszcza w przypadku korzystania z sieci intranet lub sieci. W Register.com v. Verio, Inc. pobieranie danych z bazy danych WHOIS, po zapoznaniu się z warunkami użytkowania, było przyjęciem tych warunków, nawet jeśli nie było kliknięć. Te przykłady pokazują, że warunki użycia, odpowiednio ustawione, mogą być wiążące dla użytkownika. Aktywny program bezpieczeństwa rozpoczyna się od przeglądu umów, licencji i warunków użytkowania we wszystkich relacjach z organizacją. To, że nie istniało porozumienie umowne, nie oznacza, że nie można go utworzyć poprzez odpowiednie powiadomienie o warunkach umowy i zachowaniu, które wykazują zgodę na te warunki. Takie umowy są pierwszą linią obrony specjalisty ds. Bezpieczeństwa. Dają możliwość ograniczenia ryzyka z pracownikami organizacji, kontrahentami, dostawcami i podmiotami stowarzyszonymi. Mając to na uwadze, rozdział ten porusza kwestie, które pojawiają się w dużej mierze poza warunkami ochrony kontraktowej, a także sugeruje dodatkowe potencjalne środki zaradcze w ramach samopomocy.

PRAWA WŁASNOŚCI I TAJEMNICE HANDLOWE.

Przez wiele lat, chyba że pomysł był opatentowany, podstawową ochroną wewnętrznych danych biznesowych, poufnych lub zastrzeżonych informacji i kodu komputerowego była doktryna prawa zwyczajowego tajemnic handlowych. Ogólnie rzecz biorąc, tajemnicę handlową można uznać za dowolne wewnętrzne, niepublikowane know-how dotyczące produkcji, rysunki, wzory lub informacje o sprzedaży wykorzystywane w handlu lub przedsiębiorstwie, które mają zastosowanie komercyjne i które zapewniają firmie pewną przewagę strategiczną. Takie informacje, o ile były (a) nie publikowane ani rozpowszechniane wśród innych osób, które nie były zobowiązane do zachowania poufności, oraz (b) utrzymywane w tajemnicy wraz z organizacją chroniącą, mogłyby być chronione jako tajemnica handlowa. Prawo tajemnicy handlowej uznaje zatem własność firmy lub jej własność w takich informacjach, danych lub procesach. Istnieją jednak istotne ograniczenia praktyczne w stosowaniu ochrony tajemnicy handlowej. Przede wszystkim, w przypadku każdego produktu sprzedawanego na rynku, prawo nie chroni konkurenta widzącego produkt, a następnie używa go, aby dowiedzieć się, jak wytwarzać podobne lub podobne produkty. Konkurenci mają zatem swobodę inżynierii wstecznej produktu, o ile wykonywana jest inżynieria odwrotna całkowicie niezależnie. Drugim zastrzeżeniem jest to, że organizacja musi udowodnić nie tylko, że informacje kwalifikują się do ochrony tajemnicy handlowej, ale także, że chroniły tajemnicę informacji zgodnie z prawem obowiązującej jurysdykcji. Oznacza to, że własność nie będzie rejestrowana, ale będzie rozpatrywana indywidualnie, co sprawi, że egzekwowanie ochrony tajemnicy handlowej będzie czasochłonne i kosztowne. Zasadniczo wymagany dowód polega na wykazaniu, że istniał aktywny program bezpieczeństwa, który był

wystarczający aby chronić informacje jako poufne. Różne programy można uznać za odpowiednie, w zależności od okoliczności, ale zazwyczaj takie programy mają pięć wspólnych zasad:

1. Spis informacji o tajemnicy handlowej, które są okresowo aktualizowane

2. Program bezpieczeństwa w celu ochrony omawianej technologii, często na podstawie niezbędnej wiedzy z wyraźnym oznaczeniem informacji jako „poufne, ograniczony dostęp"

3. Pisemny opis programu ochrony, który jest udostępniany wszystkim pracownikom

4. Urzędnik egzekucyjny lub procedura nadzoru

5. Program egzekwowania prawa, w tym, jeśli to konieczne, spory sądowe w celu nakazania nieuprawnionego dostępu lub dystrybucji

W dziedzinie informatyki zasady te często oznaczają, że kod źródłowy lub inne czytelne formaty powinny być zabezpieczone w zablokowanym pliku i oznaczone jako POUFNE. Wszystkie reprezentacje kodu przechowywane na nośniku magnetycznym lub innym powinny być oznaczone jako POUFNE i zabezpieczone. Skomputeryzowane informacje powinny być chronione hasłem z ograniczeniami dotyczącymi obiegu hasła i okresowych zmian hasła. Powiadomienie o poufności powinno zostać wyświetlone natychmiast po uzyskaniu dostępu do programu, z odpowiednimi ostrzeżeniami o ograniczeniu użytkowania. Poziomy dostępu powinny być kontrolowane, tak aby uprawnienia do kopiowania, czytania i pisania były odpowiednio ograniczone. Nadzór wpisów i logowania powinien być rutynowo przeprowadzany w celu sprawdzenia, czy nie doszło do nieuprawnionego wejścia. Wreszcie należy przeprowadzać okresowe audyty w celu przetestowania i uzasadnienia procedur bezpieczeństwa. Przez wiele lat każde państwo rozwinęło własną markę ochrony tajemnicy handlowej poprzez zmieniające się orzeczenia sądowe, które ustanawiają w tym kraju coś, co nazywa się prawem zwyczajowym, w odróżnieniu od aktów ustawodawczych ustawy dotyczącej ten sam problem. W 1985 r. Ustawa o jednolitych tajemnicach handlowych (UTSA) została ogłoszona przez Krajową Konferencję Komisarzy ds. Jednolitych Praw Państwowych, z jednym z jej celów, aby ujednolicić prawa i środki zaradcze dostępne dla posiadacza tajemnicy handlowej. Jednak to modelowe prawo musiało zostać przyjęte przez każde państwo, zanim stało się prawem państwa. UTSA definiuje tajemnicę handlową jako informacje, w tym formułę, wzorzec, kompilację, urządzenie programowe, metodę, technikę lub proces, które: (a) czerpią niezależną wartość ekonomiczną, rzeczywistą lub potencjalną, z braku ogólnej wiedzy łatwo ustalić za pomocą odpowiednich środków przez inne osoby, które mogą uzyskać wartość ekonomiczną z jego ujawnienia lub wykorzystania; oraz (b) jest przedmiotem wysiłków, które są uzasadnione w danych okolicznościach, aby zachować jego tajemnicę. Określa również bezprawne zabranie tajemnicy handlowej lub sprzeniewierzenie jako bezprawne wykorzystanie tajemnicy handlowej, w tym (a) świadome zdobycie tajemnicy za pomocą niewłaściwych środków lub (b) ujawnienie tajemnicy bez zgody.

ŚRODKI ZARADCZE W PRZYPADKU PRZYWŁASZCZENIA TAJEMNICT HANDLOWEJ

Sprzeniewierzenie tajemnicy handlowej to nieuprawnione użycie lub ujawnienie tajemnicy handlowej. W prostej mowie jest to zabranie lub kradzież. Może to być osoba, która ma powierniczy obowiązek zachowania poufności, na przykład pracownik; może to stanowić naruszenie umowy o poufności; lub podjęcie może nastąpić poprzez niewłaściwy dostęp lub środki. Sprzeniewierzenie może być potraktowane zgodnie z prawem powszechnym jako czyn niedozwolony w zakresie konwersji, naruszenia, nieuczciwej konkurencji lub ingerencji w stosunki umowne. Jak omówiono, są obecnie określone przepisy ustawowe na mocy UTSA dotyczące sprzeniewierzenia tajemnicy handlowej. UTSA przyznaje pokrzywdzonym pewne środki zaradcze, w tym nakazanie wykorzystania sprzeniewierzonej

własności, odszkodowań i opłat adwokackich. Kiedy sprzeniewierzenie jest przedmiotem fizycznym, takim jak napęd dyskowy, właściciel może zwrócić się do sądu o nakazanie zajęcia i zwrotu jego własności. Ponadto, jeżeli przywłaszczenie narusza również inne przepisy chroniące własność intelektualną, takie jak przypadki, w których naruszenie narusza prawa autorskie , właściciel nieruchomości może być uprawniony do dodatkowej ulgi. Dokładnie, jakie środki zaradcze są dostępne, będą różne w poszczególnych stanach. Co ciekawe, sama jednolitość, którą stworzyła UTSA, doprowadziła do odmiennego traktowania dostępnych roszczeń i środków zaradczych. Na przykład przed UTSA kradzież poufnych list pracodawców przez pracownika spowodowała powstanie prawa zwyczajowego za naruszenie domniemanego zobowiązania powierniczego należnego pracodawcy pracownikowi, jak również roszczenie o przywłaszczenie tajemnic handlowych. UTSA stanowi, że jej środki zaradcze wyprzedzają inne środki ochrony prawnej; innymi słowy, roszczenie na podstawie UTSA jest ważniejsze niż roszczenie z tytułu naruszenia obowiązku powierniczego, jak również roszczenie o sprzeniewierzenie tajemnic handlowych. W sądach istnieje podział na to, czy UTSA zastępuje jedynie zwykłe przyczyny powództwa o sprzeniewierzenie tajemnic handlowych lub rozciąga się na wszelkie roszczenia o odszkodowanie, które powstają w wyniku sprzeniewierzenia bez względu na to, jak zostały określone. Szerszy zasięg UTSA wydaje się być preferowany przez rosnącą większość sądów, które do tej pory rozważały tę kwestię. Z tej niepewności wynika ,że specjaliści ds. bezpieczeństwa powinni chronić tajemnice handlowe, informacje poufne i inne cenne dane poprzez warunki umowne między innymi z pracownikami, sprzedawcami i użytkownikami, aby zminimalizować zależność od UTSA. W przypadku sprzeniewierzenia, oprócz środków cywilnych, często odrębne ustawy państwowe traktują to jako kradzież i czyn przestępczy. Takie ustawy są zazwyczaj specyficzne dla państwa. Przed 1996 r. Ustawa o tajemnicy handlowej (TSA) była jedyną ustawą federalną zakazującą przywłaszczenia tajemnicy handlowej. TSA miała jednak ograniczoną użyteczność, ponieważ nie dotyczyła pracowników sektora prywatnego i zapewniała jedynie ograniczone sankcje karne. Aby przeciwdziałać wzrostowi liczby przestępstw komputerowych, Kongres uchwalił ustawę o szpiegostwie gospodarczym z 1996 r. (EEA), która zapewnia większą ochronę zastrzeżonych i gospodarczych informacji zarówno podmiotów korporacyjnych, jak i rządowych przed kradzieżą zagraniczną i krajową. EEA kryminalizuje dwie główne kategorie korporacyjne szpiegostwo: szpiegostwo gospodarcze i kradzież tajemnic handlowych. Sekcja 1831 karze tych, którzy kradną handlowe sekrety „na korzyść obcego rządu, zagranicznego podmiotu lub zagranicznego agenta". Rozdział 1832 stanowi ogólne przestępcze zastrzeżenie tajemnicy handlowej. EEA kryminalizuje kradzież, ukrywanie, niszczenie, szkicowanie, kopiowanie, przesyłanie lub otrzymywanie tajemnic handlowych bez zezwolenia lub za pomocą wiedza, że tajemnice handlowe były sprzeniewierzony. Kryminalizuje również próby i spiski w celu wykonania któregokolwiek z tych działań. EEA nakłada kary na strony odpowiedzialne za podjęcie działań, które mają na celu przyniesienie korzyści rządowi zagranicznemu z karami do 250 000 USD i karą pozbawienia wolności do 10 lat. EEA wyraźnie określa tajemnicę handlową, która obejmuje informacje przechowywane w mediach elektronicznych i obejmuje „programy lub kody, zarówno materialne, jak i niematerialne", o ile:

(a) ich właściciel podjął rozsądne środki w celu zachowania takiej informacji w tajemnicy; i

(b) informacje czerpią niezależną wartość ekonomiczną, rzeczywistą lub potencjalną, z faktu, że nie są powszechnie znane i nie można ich łatwo ustalić za pomocą odpowiednich środków przez społeczeństwo

Chociaż można założyć, że ta definicja jest stosunkowo prosta, nie wszystko jest takie, jak się wydaje. W przypadku kradzieży tajemnicy handlowej, Sąd Apelacyjny zbadał, co oznacza , gdy EEa mówi, że dane lub materiał „czerpią niezależną wartość ekonomiczną, rzeczywistą lub potencjalną, z braku ogólnej wiedzy i łatwo ustalić za pomocą odpowiednich środków przez opinię publiczną.

”Zauważywszy, że inni przyjęli, że słowo„ społeczeństwo ”oznaczało ogół społeczeństwa, sąd w Lange stanowczo zauważył, że tak nie jest. Ponadto standardem pomiaru osób, które mogą łatwo ustalić wartość ekonomiczną (w tym przypadku) projektu i składu zespołów hamulcowych samolotów, nie jest przeciętna osoba na ulicy, ponieważ zakłada to (jak wspomina sąd), że każda osoba potrafi zrozumieć i zastosować coś tak tajemniczego jak numer Avogadro. Zamiast tego definicja terminu „społeczeństwo” powinna uwzględniać segment populacji, który byłby zainteresowany i rozumieć naturę tego, co rzekomo zostało sprzeniewierzone. Międzynarodowy zasięg aktu jest ograniczony, wykraczający poza Stany Zjednoczone tylko wtedy, gdy: „(1) sprawca jest osobą fizyczną będącą obywatelem lub stałym rezydentem Stanów Zjednoczonych lub organizacją zorganizowaną zgodnie z prawem Stanów Zjednoczonych lub państwa lub jednostki politycznej… lub (2) czynem w celu popełnienia przestępstwa popełniono w Stanach Zjednoczonych. ”Niewielu oskarżonych zostało oskarżonych na mocy ustawy od jej wejścia w 1996 r., więc dokładny zasięg nie został jeszcze przetestowany. Język EEA stosuje jednak swoje przepisy do korporacji z siedzibą lub działalnością podlegającą jurysdykcji USA, które mogą być ścigane na mocy ustawy. Wreszcie środki odwoławcze w ramach EOG mogą być przywoływane wyłącznie przez Stany Zjednoczone. Zgodnie z ustawą nie ma prywatnego prawa do działania.

CZUJNOŚĆ TO NAJLEPSZA PRAKTYKA

Kluczowe punkty do zapamiętania to: Bezpieczeństwo i tajemnica handlowa są zawsze ze sobą powiązane. Tajemnica handlowa nie może istnieć bez takiego zabezpieczenia. Maksyma „Wieczna czujność jest ceną wolności”, często przypisywana Thomasowi Jeffersonowi, powinna w kontekście ochrony informacji biznesowych być powtórzona jako „Wieczna czujność jest ceną ochrony tajemnicy handlowej”. To nie jest tak chwytliwe wyrażenie, ale jest to cena, jaką każda firma musi zapłacić, jeśli w całości lub w części opiera się na prawie tajemnicy handlowej w celu ochrony. W takich sytuacjach największe zapewnienie ochrony można uzyskać poprzez rygorystyczne warunki umowne i forsowne egzekwowanie.

PRAWO WŁASNOŚCI INTELEKTUALNEJ I OPROGRAMOWANIE.

Ze względu na obawy dotyczące prawdziwego zakresu ochrony zapewnianej przez oprogramowanie objęte prawem patentowym i prawem autorskim, programy początkowo były chronione jako tajemnice handlowe. Taka ochrona stała się coraz bardziej problematyczne w dzisiejszym społeczeństwie, gdzie technologia informacyjna i nacisk na swobodny przepływ informacji utrudniają kontrolowanie poufności. Prawo autorskie rozwinęło się obecnie w celu włączenia programów komputerowych. Od 1964 r. Amerykańskie biuro ds. Praw autorskich zezwoliło na rejestrację programów komputerowych, chociaż orzeczenia sądowe były podzielone na temat stosowania ustawy o prawie autorskim. W 1976 r. Kongres uchwalił ustawę o prawie autorskim z 1976 r., która niewiele zrobiła, aby rozwiązać dwuznaczność. Wyjaśnienie ostatecznie uzyskano w ustawie o prawie autorskim do oprogramowania komputerowego z 1980 r., która wyraźnie rozszerzyła ochronę praw autorskich na oprogramowanie. Wszelkie prace, które można naprawić na dowolnym materialnym nośniku, mogą być chronione prawem autorskim, jako dzieła literackie oparte na autorstwie kodu źródłowego i kodu obiektu, nawet jeśli praca może być odtworzona tylko maszynowo. Ochrona praw autorskich nie chroni jednak „idei”. Raczej chroni szczególny wyraz idei. Jak widać w równoległym rozprzestrzenianiu się arkuszy kalkulacyjnych, pomysł na arkusz kalkulacyjny nie może być chroniony, ale może to być konkretny kod, który tworzy arkusz kalkulacyjny. W celu zakwalifikowania się do ochrony praw autorskich praca musi być (a) oryginalna, (b) utrwalona w materialnym medium i (c) nie tylko wcieleniem idei. Po uzyskaniu ochrony praw autorskich przyznaje właścicielowi praw autorskich wyłączne prawo do powielania, publikowania, przygotowywania prac pochodnych, rozpowszechniania, wyświetlania i wykonywania dzieła chronionego prawem autorskim. W 1990 r.

Kongres uchwalił ustawę o komputerowym wypożyczaniu oprogramowania, , która dodała do listy naruszeń praw autorskich dystrybucję programu komputerowego w celu uzyskania korzyści handlowej. Materiały chronione prawem autorskim po 1978 r. Są chronione przez mniej niż 75 lat od daty pierwszej publikacji lub 100 lat od daty utworzenia.

PRACA NA RZECZ WYNAJMU I PRAW AUTORSKICH

Prawa autorskie do utworu nie zawsze należą do osoby, która je tworzy. Najczęstszymi wyjątkami są dzieła, które wchodzą w zakres pojęcia „praca do wynajęcia". Praca do wynajęcia nie jest własnością twórcy, ale osób, które zatrudniły twórcę do stworzenia pracy. Najczęściej koncepcja ta dotyczy pracowników, którzy stworzyli pracę w ramach swojego zatrudnienia. Kluczową koncepcją jest zakres zatrudnienia. Nawet jeśli praca jest tworzona poza biurem i normalne godziny pracy, nadal będzie to praca do zatrudnienia, jeśli mieści się w zakresie zatrudnienia. Jednak praca, która nie mieści się w zakresie zatrudnienia i jest tworzona poza biurem, prawdopodobnie nie zostanie uznana za pracę do wynajęcia. Z powodu takich problemów lepszą praktyką w kontaktach z pracownikami lub niezależnymi kontrahentami jest zapewnienie specyfiki porozumienia co do tego, co jest pracą i kiedy tworzenie pracy będzie podlegać doktrynie pracy do zatrudnienia.

PRAWA AUTORSKIE WYNIKAJĄ Z UTWORZENIA DZIEŁA

Każdy, kto obejrzał dzieło objęte prawami autorskimi, prawdopodobnie zna symbol © umieszczony na opublikowanej pracy chronionej prawami autorskimi, wraz z nazwą właściciela praw autorskich oraz rokiem utworzenia lub publikacji dzieła. Przez wiele lat takie zawiadomienie było a fortiori niezbędne do ochrony praw autorskich. Obecnie jednak prawa autorskie wynikają z stworzenia dzieła chronionego prawem autorskim. Nadal dobrą praktyką jest informowanie świata o potencjalnym naruszeniu poprzez wprowadzenie formalności związanych z prawami autorskimi do samego dzieła. Ponadto należy zarejestrować pracę w United States Copyright Office, która obecnie opracowuje proces rejestracji online. Rejestracja prawa autorskiego zezwala również na dochodzenie odszkodowania ustawowego w wysokości od 500 USD do 20 000 USD za każde naruszenie, które często jest przydatne, aby zapobiec kolejnym naruszeniom, gdy nie można wykazać rzeczywistych szkód. Ponadto w niektórych jurysdykcjach może być konieczne zarejestrowanie praw autorskich w urzędzie ds. praw autorskich, zanim będzie można pozwać do ochrony praw autorskich. Zmiana ochrony praw autorskich ma interesujące zastosowania w przypadku utworów elektronicznych. Stworzenie utworu w jakiejś trwałej formie wystarczy, aby uruchomić ochronę praw autorskich. Stąd tworzenie kopii elektronicznej jest wystarczającą trwałością. Oznacza to, że wszelkie dane elektroniczne są już prawdopodobnie objęte ochroną praw autorskich w momencie ich oglądania lub otrzymywania. Tak więc, korzystając z takich informacji lub „pracy", należy uważać, aby nie naruszać potencjału prawa autorskie bez licencji.

PIERWSZE OGRANICZENIE SPRZEDAŻY

Właściciel praw autorskich ma prawo do sprzedaży lub licencjonowania dzieła. Jeśli praca zostanie sprzedana, posiadacz zasadniczo traci wszelkie prawa do kontroli odsprzedaży dzieła. Jest to znane jako pierwsza doktryna sprzedaży. Po umieszczeniu przedmiotu w handlu kolejne transfery nie mogą być ograniczone. Doktryna dotyczy tylko kopii, która została sprzedana. Nie tworzy licencji do kopiowania samego elementu. Aby uniknąć tego, co czasami może być problemem, jeśli program znajdzie się w rękach konkurenta, firmy często wolą licencjonować przedmiot zamiast go sprzedawać. Jeśli praca jest licencjonowana, przenoszone są tylko te prawa, które są zawarte w licencji. Wszelkie inne prawa własności pozostają po stronie licencjodawcy. W związku z tym naruszenie licencji daje licencjodawcy prawo do dzieła chronionego prawem autorskim do odzyskania pracy lub uniemożliwienia jej dalszego wykorzystania lub publikacji. Jeśli jednak licencja ma wszystkie

podstawowe oznaczenia sprzedaży, będzie ona traktowana jako jedna, niezależnie od etykiety. Jednym z interesujących przecięć tych dwóch zasad jest wymóg aktualizacji oprogramowania, aby była obecna stara wersja. Jako warunek udostępnienia uaktualnienia po obniżonej stawce, sprzedawca zazwyczaj wymaga, aby starsza wersja została uwierzytelniona przed zainstalowaniem nowszej wersji. Takie wymagania są legalne, ponieważ właściciel wcześniejszej wersji może zdecydować się na jej sprzedaż, ale wówczas musiałby zapłacić wyższą cenę za nowszą wersję i pracować nad ograniczeniem późniejszej sprzedaży oprogramowania od użytkownika, który oczekuje aktualizacji w przyszłości.

WYJĄTE DOWZWOLONEGO UŻYTKU

Wszelka ochrona praw autorskich jest przedmiotem dozwolonego użytku. Dozwolony użytek pozwala na korzystanie z utworu bez autoryzacji w ograniczonym celu. Ale jakie zastosowanie stanowi dozwolony użytek? Ustawa o prawie autorskim z 1976 r. Zasugerowała sądowi cztery niewyłączne czynniki:

1. Jaki jest cel i charakter zastosowania?

2. Jaki jest charakter dzieła chronionego prawem autorskim?

3. Ile wykorzystano dzieła chronionego prawem autorskim?

4. Jaki jest wpływ na potencjalny rynek pracy?

Pomimo kodyfikacji w ustawie o prawie autorskim z 1976 r., Dozwolony użytek pozostaje mglistą doktryną - sprawiedliwą zasadą rozsądku, w której każdy przypadek należy rozstrzygać na podstawie własnych faktów. Często jest błędnie cytowany i niewłaściwie stosowany. Podstawową koncepcją doktryny dozwolonego użytku jest umożliwienie publicznej dyskusji, przeglądu i debaty na temat dzieła chronionego prawem autorskim bez naruszania praw autorskich. Tak więc ustawa o prawie autorskim z 1976 r. podaje jako przykłady dozwolonego użytku, sytuacje „krytyki, komentarzy, doniesień prasowych, nauczania (w tym wielu kopii do użytku w klasie), stypendiów lub badań". Dozwolony użytek nie jest antidotum na brak licencji. Powinny być przywoływane z ostrożnością - rozumiejąc, że im więcej materiału jest używane i im bardziej komercyjny cel, tym mniej prawdopodobne jest, że sąd uzna to za stosowne. Rzeczywiście, czasami jedynym sposobem na zharmonizowanie przypadków, czy użycie jest dozwolonym sposobem, jest podjęcie decyzji, czy sąd ostatecznie postrzegał użytkownika jako „dobrego" lub „złego" faceta.

Formuły nie mogą być chronione prawami autorskimi

Istnieją ograniczenia dotyczące tego, jakie wyrażenia mogą być chronione prawem autorskim. Częstym źródłem argumentów jest to, czy ponieważ nie można ochronić pomysłu, wyrażenie jest bezpośrednio napędzane przez jego treść (tj. wyrażenie jest po prostu funkcją idei). Z tego powodu formuły nie mogą być chronione prawem autorskim. Oznacza to, że gdy formuły są częścią programu komputerowego, należy rozważyć inne sposoby obrony, takie jak tajemnica handlowa lub ewentualnie ochrona patentowa. Gdyby ujawnić formułę poprzez publikację praw autorskich, stracilibyśmy zdolność do ochrony tych informacji.

str. 11.10 11.4.6///

PRAWA AUTORSKIE NIE CHRONIĄ „WYGLĄDU I DZIAŁANIA" OPROGRAMOWANIA

Ochrona praw autorskich zwykle obejmuje fizyczną manifestację programu komputerowego w kodzie źródłowym i kodzie obiektowym. Działanie tego kodu, ponieważ przekłada się na to, co postrzega ludzki umysł, zostało opisane jako „wygląd i działanie" programu. Podejmując próbę ilościowego

określenia pojęcia „wygląd i działanie”, sądy rozważyły, czy organizacja, struktura i kolejność programu mogą być chronione. W Stanach Zjednoczonych Whelan Associates, Inc. przeciwko Jaslow Dental Lab., dało największe możliwości ochrony wyglądu. W takim przypadku żaden kod nie został skopiowany, a program działał na innej platformie. Niemniej jednak stwierdzono naruszenie praw autorskich, ponieważ skopiowano organizację, strukturę i kolejność programu. Sąd uznał, że struktura i logika programu są najtrudniejsze do stworzenia i że idea może być chroniona, ponieważ została zawarta w strukturze programu, ponieważ ze względu na różnorodność, która była możliwa, struktura niekoniecznie była tylko przedłużeniem pomysł. Od czasu Whelana sądy w Stanach Zjednoczonych wycofały się z tak szerokiej ochrony. W 1992 roku Computer Associates, Inc. przeciwko Altai, Inc. opracował tak zwany test filtracji abstrakcyjnej. Wyniki tego testu definiują jako niezabezpieczone: (a) struktury programu, które są podyktowane wydajnością operacyjną lub wymaganiami funkcjonalnymi programu i dlatego są uważane za część pomysłu i (b) wszystkie narzędzia i podprogramy, które mogą być uznane za zawarte w domenie publicznej . Należy porównać tylko to, co pozostaje, pod kątem ewentualnego naruszenia praw autorskich. Podczas gdy ochrona wyglądu i wyglądu może się różnić w zależności od poszczególnych obwodów federalnych, sądy na ogół odchodzą od szerszej ochrony. Jednak niekoniecznie musi to być prawda międzynarodowa; Wydaje się, że angielskie prawo zapewnia szerszą ochronę dzięki decyzji Whelana.

INŻYNIERIA ODWROTNA JAKO WYJĄTEK OD PRAW AUTORSKICH

W dziedzinie oprogramowania komputerowego rozważano, czy „rozbiór” w celu przeprowadzenia inżynierii wstecznej programu stanowi naruszenie praw autorskich. Wydaje się, że osobom zaangażowanym w ochronę programów komputerowych, jak również osobom zaangażowanym w konkurencyjne produkty, inżynieria odwrotna nie stanowi naruszenia, mimo że demontaż programu należy do kategorii czynów zabronionych przez ustawę o prawie autorskim z powodu doktryny dozwolonego użytku. Sąd Apelacyjny Sega Enterprises Ltd. przeciwko Accolade, Inc. stwierdził, że zgodnie z prawem:

… Gdzie dezasemblacja jest jedynym sposobem na uzyskanie dostępu do pomysłów i elementów funkcjonalnych zawartych w chronionym prawem autorskim programie komputerowym, a tam, gdzie istnieje uzasadniony powód, aby szukać takiego dostępu, dezasemblacja jest uczciwym wykorzystaniem praw autorskich.

Nie tylko Sąd Apelacyjny przeciwstawił się inżynierii odwrotnej jako roszczeniu dotyczącemu praw autorskich. Sąd Federalny doszedł do podobnego wniosku dotyczącego inżynierii odwrotnej kodu obiektowego, aby dostrzec „idee” stojące za programem w Atari Games Corp. kontra Mnemonics, Inc. na tej podstawie, że rozwinął nauki. Dodatkowo w Assessment Techs. of WI, LLC, v. WIREData, Inc., inny Sąd Apelacyjny oparł się na Sega i ustalił, że WIREData, Inc. może wyodrębnić dane niechronione prawem autorskim z programu komputerowego chronionego prawem autorskim, zauważając, że celem ekstrakcji było uzyskanie surowych danych, a nie konkurować z Assessment Technologies, sprzedając kopie samego programu. W Evolution, Inc. przeciwko SunTrust inny Sąd opierał się zarówno na Sega, jak i WIREData, gdy zezwalał pozwanemu na skopiowanie części kodu źródłowego powoda w celu wyodrębnienia nieuprawnionych danych z praw autorskich program komputerowy. Tak więc, o ile nie podejmie się starannego rozważenia zastosowania ochrony praw autorskich, jedynie prawo autorskie do oprogramowania niekoniecznie będzie chroniło przed naśladownictwem.

INTERFEJSY

Istnieje otwarty problem dotyczący tego, czy prawa autorskie chronią format komunikacji między aplikacją a danymi. Konkurenci, szczególnie w dziedzinie gier, szukają inżynierii odwrotnej formatu interfejsu, aby nowe moduły były kompatybilne z istniejącym sprzętem. Taka inżynieria odwrotna nie

narusza praw autorskich, o ile nowy produkt nie wyświetla obrazów chronionych prawem autorskim ani innych wyrażeń chronionych prawami autorskimi. Tak więc niechroniony interfejs może być chroniony, jeśli takie obrazy lub wyrażenia chronione prawem autorskim są osadzone na wyświetlaczu.

ZASTOSOWANIA TRANSFORMACYJNE

Jednym z czynników, które uważa doktryna dozwolonego użytku, jest „ilość i istotność części wykorzystywanej w odniesieniu do dzieła chronionego prawem autorskim jako całości". W praktyce oznacza to, że sądy przyglądają się, ile zostało pobrane i w jakim celu . Można wziąć trochę, ale wciąż brać istotę programu. Można też wziąć trochę tego, czego nie próbowano powielać, a raczej używać materiału chronionego prawem autorskim jako trampoliny dla nowego dzieła. Z tego jakościowego i ilościowego badania wynika pojęcie transformacyjnego wykorzystania, które stało się monetą analizy w decyzji Sądu Najwyższego z 1994 r. w sprawie Campbell przeciwko Acuff-Rose Music, Inc. rapowej parodii popularnej piosenki. Tam, kierując się wskazówkami z początkowego języka sekcji 107 kodyfikującego dozwolony użytek, Sąd Najwyższy zapytał, czy „nowa" praca „dodaje coś nowego, z innym celem lub innym charakterem, zmieniając pierwszy z nowym wyrażeniem, znaczeniem lub wiadomością; innymi słowy, pyta, czy i w jakim stopniu nowa praca ma charakter transformacyjny "

„Chociaż takie przekształcające użycie nie jest absolutnie konieczne do stwierdzenia dozwolonego użytku,… cel praw autorskich, promowanie nauki i sztuki, jest generalnie wspierany przez tworzenie dzieł transformacyjnych. Takie prace leżą więc u podstaw gwarancji uczciwego użycia doktryny oddychając przestrzenią w ramach praw autorskich… i im bardziej transformująca jest nowa praca, tym mniejsze będzie znaczenie innych czynników, takich jak komercjalizacja, które mogą być sprzeczne ze stwierdzeniem dozwolonego użytku."

W związku z tym przekształcające wykorzystanie może odgrywać rolę wcześniejszego prawa autorskiego i nadal nie być uważane za naruszenie, o ile powstałe nowe dzieło jest właśnie takie - nowe.

PRACE POCHODNE

Zgodnie z sekcją 106 (2) ustawy o prawie autorskim z 1976 r. Właściciel praw autorskich ma wyłączne prawo „do przygotowywania dzieł pochodnych w oparciu o dzieło objęte prawem autorskim". Ustawa definiuje „dzieło pochodne" jako:

… Dzieło oparte na jednym lub kilku wcześniejszych utworach, takich jak tłumaczenie, aranżacja muzyczna, dramatyzacja, fabularyzacja, wersja filmowa, nagrywanie dźwięku, reprodukcja dzieł sztuki, skrócenie, kondensacja lub inna forma, w której dzieło może zostać przekształcone , przekształcone lub przystosowane. Praca składająca się z wersji redakcyjnych, adnotacji, opracowań lub innych modyfikacji, które jako całość stanowią oryginalne dzieło autorstwa, jest „pracą pochodną".

„Praca pochodna" jest zatem definiowana jako oryginalne dzieło, które jest niezależnie chronione prawem autorskim. Aby naruszyć wyłączne prawo do przygotowania dzieła pochodnego przyznanego przez ustawę o prawie autorskim właścicielowi praw autorskich, sprawca naruszenia nie musi w rzeczywistości skopiować oryginalnego utworu, ani nawet nie utrwalić w materialnym środku wyrazu dzieła rzekomo naruszającego prawo. Dlatego też prawo do tworzenia pracy pochodnej może być użytecznym narzędziem w równoważeniu prób pirackich programów komputerowych i kwestii dozwolonego użytku. Ustawa o prawie autorskim tworzy wyłączenie dla prawowitego właściciela zakupionej licencji na program komputerowy do adaptacji programu chronionego prawem autorskim, jeśli rzeczywista adaptacja „jest tworzona jako istotny krok w wykorzystaniu programu komputerowego w połączeniu z maszyną i jest używana w żaden inny sposób. "Adaptacja nie może zostać przeniesiona na stronę trzecią. Prawo do adaptacji jest w istocie prawem do modyfikowania lub,

w języku aktu, tworzenia pracy pochodnej. Takie zmiany mogą być wprowadzone nawet bez zgody właściciela oprogramowania, o ile takie modyfikacje są używane tylko wewnętrznie i są niezbędne do dalszego korzystania z oprogramowania

Semiconductor Chip Protection Act z 1984 r.

Semiconductor Chip Protection Act z 1984 r. (SCPA) chroni w ramach ustawy o prawie autorskim „prace maski utrwalone w produkcie półprzewodnikowym". SCPA chroni nie sam produkt, ale kopiowanie projektu obwodu lub planu. Z powodu inżynierii odwrotnej ochrona zapewniana przez SCPA jest w praktyce ograniczona.

BEZPPOŚREDNIE , SKŁADKOWE LUB ZASTĘPCZE NARUSZENIE

Naruszenie praw autorskich zazwyczaj wymaga wykazania znacznego podobieństwa między rzekomo obrażającym użyciem a chronionym wyrażeniem zawartym w utworze. Naruszenie może nastąpić poprzez zwykłą czynność drukowania (bez zezwolenia), poprzez opublikowanie w Sieci lub innej formie nieautoryzowanego rozpowszechniania, poprzez utworzenie dzieła pochodnego lub przez inną czynność, która koliduje z prawami właściciela praw autorskich. Prawa autorskie mogą być naruszane bezpośrednio, partycypacyjnie lub zastępczo. Bezpośrednie naruszenie to termin przypisany aktorowi, który narusza prawa autorskie. Naruszenie prawa do udziału wiąże się ze świadomym zapewnieniem środków, aby naruszenie mogło nastąpić. Odpowiedzialność za naruszenie składkowe może opierać się na aktywnym zachęcaniu do (lub wywoływaniu) naruszeń poprzez określone działania lub na dystrybucji produktu, który rozpowszechnia wykorzystywać do naruszania praw autorskich, jeśli produkt nie jest zdolny do znaczących "lub„ znaczących handlowo "zastosowań niezgodnych z prawem. Jednak wtórna odpowiedzialność za naruszenie praw autorskich nie istnieje w przypadku braku bezpośredniego naruszenia przez osobę trzecią. Paskudne naruszenie ma miejsce, gdy ktoś jest odpowiedzialny za działania innego, który narusza naruszenie. Zazwyczaj jest to sytuacja pracodawcy odpowiedzialnego za czyny pracownika. Nie wszystkie sytuacje przyznają się do prostych odpowiedzi, np. gdy osoba popełnia bezpośrednie naruszenie, faktycznie kserując dzieło. Nowe technologie nieustannie stwarzają problemy co do tego, czy doszło do naruszenia i czy naruszenie narusza interes publiczny. Ogólnie rzecz biorąc, w obliczu problemu potencjalnego naruszenia praw autorskich należy zadać następujące pytania:

* Czy produkt lub usługa mogą być wykorzystywane do naruszania praw autorskich, czy też produkt jest zdolny do poważnych zastosowań niezgodnych z prawem?

* Jeśli tak, czy właściciel produktu lub usługi zachęcał użytkownika do korzystania z niego w celu naruszenia?

* Alternatywnie, czy właściciel produktu lub usługi posiadał wiedzę na temat konkretnego wykorzystania naruszającego prawo i ma możliwość zapobiegania?

Dzisiaj przyjmujemy dostawców usług internetowych (ISP) za pewnik. Jednak zastosowanie tych pytań początkowo doprowadziło sądy do stwierdzenia, że dostawcy usług internetowych ponoszą odpowiedzialność za naruszenie składek. Na przykład strona internetowa zachęcająca i ułatwiająca przesyłanie materiałów chronionych prawami autorskimi okazała się bezpośrednim naruszeniem praw autorskich właściciela, mimo że dostawca faktycznie nie dokonał przesyłania. który został opublikowany na swoim serwerze i nie poprawił go, może zostać uznany za odpowiedzialnego za naruszenie. W swojej mądrości Kongres, w Digital Millennium Copyright Act (DMCA), stworzył bezpieczną przystań dla dostawców usług internetowych, aby kwestia polityki publicznej, dostawca

usług internetowych nie musi monitorować każdej transmisji pod kątem potencjalnego naruszenia praw autorskich.

Środki odwoławcze w sprawach cywilnych i karnych

Ustawa o prawie autorskim zawiera kilka sekcji, które w szczególności odnoszą się do kar i środków zaradczych za naruszenie. Obejmują one nakaz sądowy (tj. nakaz sądowy kończący postępowanie naruszające prawo), konfiskatę i pozbywanie się artykułów naruszających prawo, odszkodowań, kosztów postępowania sądowego i honorariów adwokackich, i sankcji karnych. dostępne, warto wspomnieć o kilku. Ogólnie rzecz biorąc, właściciel praw autorskich musi wybrać między rzeczywistymi stratami (tj. tym, co faktycznie stracił, a wszelkimi zyskami osiągniętymi przez sprawcę naruszenia) i odszkodowaniami ustawowymi. Rzeczywiste odszkodowania oznaczają straty gospodarcze faktycznie poniesione w wyniku naruszenia. Rodzaje rzeczywistych szkód, które zostały przyznane, obejmują koszty rozwoju oprogramowania, konsekwencje ekonomiczne utraconych klientów, utraconą przyszłą sprzedaż, wartość opłat licencyjnych naruszających prawo, w przypadku gdy licencjodawca jest wykluczony ze sprzedaży rynkowej, utraconą wartość rynkową naruszonego materiału oraz utracone opłaty licencyjne. Nadmierne szkody rzeczywiste nie są automatyczne; na posiadaczu licencji spoczywa ciężar udowodnienia, że działalność naruszająca prawo i straty ekonomiczne są ze sobą powiązane przyczynowo, w którym to momencie strona naruszająca prawo musi wykazać, że posiadacz licencji i tak poniósłby stratę. Właściciel praw autorskich może zdecydować się na otrzymanie odszkodowania ustawowego, a nie rzeczywistego odszkodowania i zysków naruszającego. Dokonanie wyboru jest obowiązkowe i musi zostać dokonane przed wprowadzeniem ostatecznego wyroku. Po dokonaniu wyborów jest ostateczny. Odszkodowania ustawowe wynoszą zazwyczaj od 500 do 20 000 USD „za wszystkie naruszenia związane z działaniem, w odniesieniu do każdej pracy, za którą każdy lub więcej sprawców naruszeń ponosi odpowiedzialność solidarną.… Dla celów niniejszej sekcji wszystkie części kompilacja lub praca pochodna stanowią jedną pracę. ”Kwota ta może zostać zwiększona do 100 000 USD, jeśli sąd uzna, że naruszenie było umyślne i zredukowane do 200 USD, jeśli sąd uzna, że sprawca naruszenia„ nie wiedział i nie miał powodu sądzić ”, że czyn było naruszeniem. Teoretycznie odszkodowania ustawowe mają na celu zbliżenie rzeczywistych poniesionych szkód i zostały opracowane jako alternatywny system odszkodowań dla właścicieli praw autorskich, gdy rzeczywiste szkody są trudne do obliczenia. Przy ustalaniu, czy wybrać faktyczne czy odszkodowania ustawowe, właściciel praw autorskich powinien przeprowadzić dokładną analizę w celu ustalenia, ile oddzielnych naruszeń miało miejsce, uzasadniających na podstawie statutu odrębne nagrody. Mimo że umieszczanie różnych programów komputerowych chronionych prawem autorskim na tablicy ogłoszeń w celu pobrania stanowi wiele naruszeń, co powoduje wielokrotność kopii tej samej postaci z kreskówek w różnych pozach stanowią jedno naruszenie, ponieważ skopiowano tylko jedną pracę. Jak wspomniano, jest to jeden z ustawowych systemów, które zniechęcają do błahych spraw sądowych, nakładając koszty postępowania sądowego na stronie przegrywającej. Statut zezwala stronie zasadniczo dominującej na odzyskanie rozsądnych opłat i kosztów adwokackich od strony przegrywającej. Kto jest stroną przeważającą i co stanowi rozsądne honoraria adwokackie są odrębnymi i odrębnymi kwestiami, które będą rozstrzygane przez sądy. Naruszenie praw autorskich może być również ścigane karnie i zazwyczaj wymaga demonstracji złej woli lub zamiaru. Jedno lub więcej naruszeń o łącznej wartości detalicznej przekraczającej 1000 USD w ciągu 180 dni lub „w celu uzyskania korzyści handlowej lub prywatnego zysku finansowego” może zostać ukarane karą pozbawienia wolności od jednego roku do pięciu lat. Nawet bez wykazania motywu zysku finansowego, 10 lub więcej naruszeń o wartości przekraczającej 2500 USD może skutkować do trzech lat więzienia i grzywny. Powtarzające się naruszenia pociągają za sobą sztywniejsze kary. Wreszcie, kto świadomie pomaga lub narusza prawo autorskie, podlega również postępowaniu karnemu.

DIGITAL MILLENNIUM COPYRIGHT ACT

W 1998 r. Kongres uchwalił ustawę Digital Millennium Copyright Act (DMCA) w celu rozwiązania problemów związanych z Internetem i prawami autorskimi w kontekście naszego coraz bardziej technologicznego społeczeństwa. DMCA tworzy cywilny środek zaradczy za jego naruszenie, a także sankcje karne począwszy od października 2000 r. Jednym z celów DMCA jest ochrona integralności informacji o prawach autorskich. Usunięcie informacji o prawach autorskich lub rozpowszechnienie informacji o tym, że takie prawa autorskie zostały usunięte, jest teraz możliwe do zastosowania.

KRYMINALNE ŚRODKI TECHNOLOGICZNE

Artykuł 11 Traktatu o prawie własności intelektualnej Światowej Organizacji Własności Intelektualnej wymagał od wszystkich państw sygnatariuszy zapewnienia odpowiedniej ochrony prawnej i środków zaradczych przeciwko obchodzeniu środków technicznych mających na celu zabezpieczenie praw autorskich. W odpowiedzi Kongres przyjął sekcję 1201 ustawy DMCA, która generalnie zabrania działania polegającego na obchodzeniu i handlu technologią umożliwiającą obchodzenie, środków ochrony mających na celu kontrolę dostępu do dzieł chronionych prawem autorskim. DMCA, jeśli obejdzie się „środek technologiczny, który skutecznie kontroluje dostęp do pracy chronionej" przez ustawę o prawie autorskim. „Produkcją, importem, oferowaniem społeczeństwu, zapewnianiem lub w inny sposób ruchem w jakiejkolwiek technologii jest przestępstwem cywilnym produkt, usługa, urządzenie, komponent lub jego część ", które„ są głównie zaprojektowane lub wyprodukowane w celu obejścia środka technologicznego, który skutecznie kontroluje dostęp do dzieła chronionego "na mocy ustawy o prawie autorskim. Środek technologiczny skutecznie kontroluje dostęp do utworu, jeżeli środek „w zwykłym toku jego działania wymaga zastosowania informacji lub procesu lub traktowania, z upoważnieniem właściciela praw autorskich, w celu uzyskania dostępu do utworu". Można obejść taki środek technologiczny, jeśli używa się środków „do odszyfrowania zaszyfrowanej pracy, do odszyfrowania zaszyfrowanej pracy lub w inny sposób do uniknięcia, obejścia, usunięcia, dezaktywacji lub osłabienia środka technologicznego" bez upoważnienia właściciela praw autorskich. W RealNetworks, Inc. kontra Streambox, Inc. Streambox dystrybuował oprogramowanie, które umożliwiało użytkownikom ominięcie procesu uwierzytelniania stosowanego przez RealNetworks, który dystrybuuje treści audio i wideo przez Internet. Dzięki temu użytkownicy Streambox mogą czerpać korzyści z transmisji strumieniowej audio i wideo RealNetworks bez rekompensowania właścicielom praw autorskich. Sąd Okręgowy Stanów Zjednoczonych w stanie Waszyngton stwierdził, że oprogramowanie Streambox było środkiem technologicznym, którego celem było obejście środków kontroli dostępu i kopiowania mających na celu ochronę praw autorskich właściciele. W przypadku szyfrowania cyfrowego dysku wideo (DVD) Sąd Okręgowy w Nowym Jorku nakazał umieszczanie linków do stron, na których użytkownicy mogą pobrać program deszyfrujący jako handel technologią obchodzenia i naruszenie DMCA. W Universal City Studios, Inc. przeciwko Reimerdes sąd odrzucił argument, że korzystanie z oprogramowania deszyfrującego stanowi swobodną ekspresję chronioną przez Pierwszą Poprawkę do Konstytucji Stanów Zjednoczonych. W odwołaniu wnoszący odwołanie twierdził, że nakaz naruszył Pierwszą Poprawkę, ponieważ kod komputerowy był mową, był uprawniony do pełnej ochrony i nie był w stanie przetrwać ścisłej kontroli nad chronioną mową. Sąd apelacyjny uznał, że kod komputerowy użyty w programie była chroniony mową:

Komunikacja nie traci konstytucyjnej ochrony jako „mowy" tylko dlatego, że jest wyrażona w języku kodu komputerowego. Wzory matematyczne i partytury muzyczne są zapisywane w „kodzie", tj. notacje symboliczne nie są zrozumiałe dla niewtajemniczonych, a jednak obie są objęte Pierwszą Poprawką. Gdyby ktoś zdecydował się napisać powieść w całości w komputerowym kodzie obiektowym, używając ciągów 1 i 0 dla każdej litery każdego słowa, wynikowa praca nie byłaby różna dla celów konstytucyjnych, niż gdyby była napisana w języku angielskim. Wersja „kodu obiektowego"

byłaby niezrozumiała dla czytelników spoza społeczności programistycznej (i nudna do czytania nawet dla większości społeczeństwa), ale nie byłaby bardziej niezrozumiała niż dzieło napisane w sanskrycie dla osób niezaznajomionych z tym językiem. Niekwestionowane dowody wskazują, że nawet czysty kod obiektowy może być i często jest odczytywany i rozumiany przez doświadczonych programistów. A kod źródłowy (na dowolnym z jego różnych poziomów złożoności) może być odczytany przez wiele innych. Patrz Universal I, 111 F. Supp. 2d na 326. Ostatecznie jednak łatwość zrozumienia dzieła nie ma znaczenia dla dochodzenia konstytucyjnego. Jeśli kod komputerowy można odróżnić od mowy konwencjonalnej dla celów Pierwszej Poprawki, to nie dlatego, że jest napisany w niejasnym języku. Sąd przeanalizował następnie rodzaj kontroli, która powinna być stosowana, gdy ograniczenie jest neutralne pod względem treści:

„Po stwierdzeniu, że kod komputerowy przekazujący informacje jest „mową" w rozumieniu Pierwszej Poprawki, rozważamy w ograniczonym zakresie zakres ochrony, z której korzysta kod. Jak uznał Sąd Rejonowy, Universal I, 111 F. Supp. 2d w 327, zakres ochrony mowy zależy na ogół od tego, czy ograniczenie jest narzucone ze względu na treść wypowiedzi. Ograniczenia oparte na treści są dopuszczalne tylko wtedy, gdy służą interesującym interesom państwa i robią to za pomocą najmniej restrykcyjnych dostępnych środków. Patrz Sable Communications of California, Inc. przeciwko FCC, 492 U.S. 115, 126, 106 L. Ed. 2d 93, 109 S. Ct. 2829 (1989). Ograniczenie neutralne pod względem treści jest dopuszczalne, jeśli służy znacznemu interesowi rządu, zainteresowanie nie jest związane z tłumieniem swobodnej wypowiedzi, a regulacja jest ściśle dostosowana, co „w tym kontekście wymaga ... że wybrane środki nie obciążają znacznie więcej mowa niż jest to konieczne dla dalszego uzasadnionego interesu rządu. Turner Broadcasting System, Inc. przeciwko FCC, 512 U.S. 622, 662, 129 L. Ed. 2d 497, 114 S. Ct. 2445 (1994) (cytując Warda v. Rock Against Racism, 491 U.S. 781, 799, 105 L. Ed. 2d 661, 109 S. Ct. 2746 (1989))."

Stwierdzenie, że interes rządu w zapobieganiu nieautoryzowanemu dostępowi do zaszyfrowanych materiałów chronionych prawem autorskim jest bezspornie znaczący, oraz że regulacja programów deszyfrujących służyła temu interesowi, sąd apelacyjny utrzymał w mocy zakazy zarówno publikowania, jak i łączenia się z programem deszyfrowania. Jednak nie wszystkie wysiłki zmierzające do „obejścia" ograniczeń wchodzą w zakres zakazów DCMA. W I.M.S. Inquiry Mgmt Sys. v. Berkshire Info. Sys., Pozwany użył ważnego hasła dostarczonego własnym klientom i identyfikator użytkownika, aby zobaczyć system e-Basket powoda dokładnie tak, jak mógł to zrobić sam klient. Sąd doszedł do wniosku, że choć może to być postrzegane jako środek technologiczny, nie chodziło o obejście ściany cyfrowej w rozumieniu DCMA.

WYJĄTKI OD ZAKAZÓW DOTYCZĄCYCH OBCHODZENIA TECHNOLOGII

DMCA jednoznacznie wyodrębnia jednak wszelką obronę przeciwko naruszeniom praw autorskich, w tym doktrynę dozwolonego użytku, która nie została naruszona przez przejście DMCA. W niektórych okolicznościach dozwolony użytek może obejmować inżynierię odwrotną.

DOZWOLONY UŻYTEK I INŻYNIERIA ODWROTNA

W ten sposób można nadal szpiegować za pomocą inżynierii odwrotnej bez narażania się na ochronę praw autorskich lub DMCA. Jednak w sprawie Bowers przeciwko Baystate Technologies, Inc. podzielony Federalny Sąd Apelacyjny uznał, że licencja na pakowanie w folię termokurczliwą zakazująca inżynierii odwrotnej była wykonalna w stosunku do licencjobiorcy, który dokonał odwrotnej inżynierii zestawu narzędzi Designer Bowers w celu opracowania konkurencyjnego produktu. Sąd uznał, że język umowny przewyższył „dozwolony użytek" dozwolony na mocy ustawy o prawie autorskim. Piąty Wydział osiągnął odwrotny skutek we wcześniejszej decyzji Vault Corp. v. Quaid Software, Ltd., stwierdzając w szczególności, że ustawa o prawie autorskim ma pierwszeństwo przed

prawem państwowym, które usiłuje zakazać demontażu i nie może egzekwować umowy licencyjnej na masową dystrybucję. Zatem zakres, w jakim Bowers może być przestrzegany, jest nadal niejasny, ale wydaje się, że jest kwestionowany w kolejnych decyzjach. Bowers sugeruje kurs, który przedsiębiorstwa mogą podjąć w celu ograniczenia inżynierii odwrotnej, czyli ograniczenia tego prawa na podstawie umowy. Jeśli Bowers zostanie powszechnie zaakceptowany, Stany Zjednoczone będą w tej kwestii pozostawać w konflikcie z Unią Europejską. W swojej dyrektywie w sprawie oprogramowania z 1991 r. Unia Europejska ustanowiła prawo do inżynierii wstecznej, która jest zgodna z „dozwolonym użytkowaniem" zgodnie z ustawą o prawie autorskim. Dyrektywa w sprawie oprogramowania przewidywała również, że prawa nie można zrzec się na podstawie umowy. Tak więc, dopóki Bowers nie zostanie rozstrzygnięty, jeśli licencja na obkurczanie zabrania inżynierii odwrotnej, najlepiej rozważyć podjęcie takiej działalności za granicą

INNE WYJĄTKI

DMCA tworzy również ważny wyjątek, który uznaje prawo do inżynierii wstecznej, jeżeli (a) osoba zgodnie z prawem uzyskała prawo do używania kopii programu komputerowego oraz (b) jedynym celem obchodzenia środka technologicznego jest identyfikacja i analiza „tych elementów programu, które są niezbędne do osiągnięcia interoperacyjności niezależnie utworzonego programu komputerowego z innymi programami". DMCA tworzy podobne wyłączenie dla obchodzenia w celu „umożliwienia interoperacyjności niezależnie stworzonego programu komputerowego z innymi programami, jeżeli takie środki są konieczne do osiągnięcia takiej interoperacyjności". Termin „interoperacyjność" jest zdefiniowany w celu objęcia „zdolności programy komputerowe do wzajemnej wymiany informacji i takich programów w celu wykorzystania wymienianych informacji. "Informacje uzyskane w wyniku tych dozwolonych aktów obchodzenia mogą być również przekazywane stronom trzecim, o ile są one wykorzystywane wyłącznie do tych samych celów. dopuszczalne w ramach tych zwolnień, jednak „tylko w takim zakresie, w jakim nie stanowi to kopii naruszeniA. "Dwie sprawy, Chamberlain Group, Inc. przeciwko Skylink Techs., Inc., i Lexmark Int'l, Inc. v. Static Control Components, Inc., są szczególnie pouczające. W obu przypadkach sądy zezwoliły konkurentowi na dostęp i inżynierię wsteczną w ramach tego zwolnienia. Natomiast w Storage Tech Corp. v. Custom Hardware Engineering Consulting, Inc. pozwany pominął ochronny klucz dostępu, aby uruchomić program diagnostyczny, kopiując kod do pamięci o dostępie swobodnym (RAM) urządzenia dostępowego pozwanego. Sąd stwierdził, że to kopiowanie stanowiło naruszenie. Wynik został odwrócony w decyzji 2 do 1 w amerykańskim obwodzie federalnym na podstawie odczytu sekcji 117 (a) i (c) ustawy DMCA, która zezwala na kopiowanie w celach konserwacyjnych. Ten ciąg decyzji doprowadził do wydania zaleceń, że dostęp jest kontrolowany za pomocą metody, która spowodowałaby naruszenie praw autorskich i że dostęp chroni nie tylko program chroniony prawem autorskim, ale dane chronione prawem autorskim, aby wykluczyć uzasadnienie Federalnego Okręgu. Sugerowano, że niektóre części kodu wykonywalnego chronionego prawem autorskim będą szyfrowane i że wymagany będzie klucz deszyfrujący, który utworzy kopię kodu i chronionych danych w ramach procesu, aby stworzyć argument naruszenia praw autorskich. Tego rodzaju zalecenia pozostają niesprawdzone, a prostszy kurs może być kontrolowany za pomocą terminów zawartych w umowie licencyjnej. Zwolnione z DMCA są także akty „dobrej wiary" polegające na obchodzeniu, w których celem są badania nad szyfrowaniem. Dopuszczalny akt badań nad szyfrowaniem wymaga, aby (a) osoba, która zgodnie z prawem uzyskała kopię, (b) czynność była konieczna do przeprowadzenia badań, (c) w dobrej wierze podjęto starania o uzyskanie zezwolenia przed obejściem, oraz (d) taki akt nie stanowi naruszenia w ramach innej sekcji ustawy o prawie autorskim lub ustawy o oszustwach komputerowych i nadużyciach z 1986 r. Z zastrzeżeniem, że musi to być akt dobrej wiary w szyfrowanie, środki technologiczne do obejścia mogą być zapewnione inni, którzy współpracują przy takich badaniach. Problem badań szyfrowania w dobrej wierze dotyczy tego, co stało się z informacjami

pochodzącymi z badań. Jeśli zostałoby ono rozpowszechnione w sposób, który mógłby pomóc w naruszeniu, w przeciwieństwie do racjonalnie obliczonego, aby przyspieszyć rozwój technologii szyfrowania, akt nadal nie wchodzi w zakres wyłączenia. Inne czynniki, które wpływają na określenie dobrej wiary, to to, czy osoba prowadząca badanie jest przeszkolona, doświadczona lub zaangażowana w badania nad szyfrowaniem i czy badacz dostarcza właścicielowi praw autorskich kopię wyników. DMCA ma również uprzedzenia wobec gromadzenia lub rozpowszechniania danych osobowych. Dlatego nie jest naruszeniem DMCA obchodzenie środka technologicznego, który zasadniczo chroni, zbiera lub rozpowszechnia informacje pozwalające na identyfikację osobową, pod warunkiem że omijanie nie przynosi żadnego innego skutku, i pod warunkiem, że sam program nie zawiera wyraźnego ostrzeżenia przed zbieraniem takich informacji oraz środków zapobiegających lub ograniczających takie gromadzenie. Krótko mówiąc, można wyłączyć pliki cookie, jeśli sam program nie zezwala na to użytkownikowi. Wreszcie, o ile dotyczy to tego rozdziału, DMCA wyklucza również ze swojego zakresu „testy bezpieczeństwa". DMCA udziela pozwolenia na przeprowadzenie testów bezpieczeństwa, które, ale dla tego zezwolenia, naruszają warunki DMCA. Jeśli z jakiegoś powodu testy bezpieczeństwa naruszyły inne przepisy ustawy o prawie autorskim lub ustawy o oszustwach komputerowych i nadużyciach z 1986 r., Nadal jest to akt naruszenia. DMCA bierze pod uwagę, czy doszło do naruszenia i przez kogo informacje zostały wykorzystane. Czynniki, które należy wziąć pod uwagę, obejmują informacje, które wykorzystano w celu promowania bezpieczeństwa właściciela lub operatora sieci komputerowej lub systemu komputerowego, jeśli został on udostępniony deweloperowi, i jeśli został wykorzystany w sposób, który nie ułatwiłby naruszenia. Dla celów DMCA, testowanie bezpieczeństwa oznacza dostęp do pojedynczego komputera lub sieci w celu „testowania w dobrej wierze, badania lub korygowania, luki w zabezpieczeniach lub podatności, za zgodą właściciela lub operatora.

ŚRODKI ZARADCZE

Sankcje karne za naruszenie DMCA mogą być dość surowe. Jeśli naruszenie jest umyślne ze względu na korzyści komercyjne, pierwsze wykroczenie pociąga za sobą karę do 500 000 USD lub 5 lat pozbawienia wolności. Późniejsze naruszenia pociągają za sobą grzywny w wysokości do 1 miliona dolarów lub 10 lat pozbawienia wolności. Środki cywilne obejmują nakaz ograniczenia naruszenia, odszkodowania za utracone zyski, odszkodowania za odzyskanie zysków naruszającego lub odszkodowania ustawowe za każde naruszenie. W zależności od sekcji danego DMCA każde naruszenie może wygenerować grzywny w wysokości do 2500 USD lub 25 000 USD. Ponieważ każdy akt naruszenia może stanowić naruszenie, ustawowe grzywny mogą stać się dość znaczące.

OCHRONA PATENTOWA.

Pomysły, które nie są chronione prawem autorskim, mogą być chronione patentem. Ogólnie rzecz biorąc, prawa patentowe chronią funkcjonalność produktu lub procesu.

OCHRONA PATENTOWA WYMAGA UJAWNIENIA

Patent można uzyskać prawidłowo, jeśli wynalazek jest nowy, użyteczny, nieoczywisty i ujawniony. Patent wymienia przyznanie wyłącznego monopolu na wynalazek w zamian za ujawnienie. Ujawnienie jest punktem wyjścia dla zdolności patentowej. Ujawnienie popiera roszczenia dotyczące zdolności patentowej (tj. Ustanawia twierdzenie, że wynalazek jest zarówno nowy, jak i nieoczywisty), a także zakres tego, co może być chronione. Zatem 35 U.S.C. sekcja 112 zapewnia:

Specyfikacja powinna zawierać pisemny opis wynalazku oraz sposób i proces jego sporządzania i używania, w takich pełnych, jasnych, zwięzłych i dokładnych warunkach, aby umożliwić każdej osobie wykwalifikowanej w dziedzinie, do której się ona odnosi, lub z którą jest prawie połączony, aby tworzyć i używać tego samego, i określa najlepszy tryb rozważany przez wynalazcę realizacji jego wynalazku.

Specyfikacja kończy się jednym lub kilkoma zastrzeżeniami, w szczególności wskazującymi i wyraźnie domagającymi się przedmiotu, który wnioskodawca uważa za swój wynalazek. [Dodano podkreślenie.]

Patent musi zatem ujawnić najlepszy sposób realizacji wynalazku, czytelny opis wynalazku, dostateczną szczegółowość, aby lekarz mógł zrozumieć i wykorzystać opis oraz odmienne zastrzeżenia, aby patent mógł zostać wydany. Dzięki odpowiedniemu ujawnieniu wynalazku wniosek informuje o technologii wykorzystywanej w patencie, aby publicznie informować o tym, co stanowiłoby naruszenie. Z perspektywy polityki publicznej ujawnienie zwiększa wiedzę publiczną. Z punktu widzenia wynalazcy kompromis to ujawnienie informacji o wyłączności. W zależności od tego, jak wynalazek ma być stosowany i obszarów, w których ochrona będzie konieczna, ujawnienie może nie być najlepszym sposobem ochrony wynalazku. Jest to szczególnie prawdziwe, jeśli wynalazca nie jest przekonany, że zostanie uznany za nieoczywisty ze stanu techniki, w którym to przypadku będzie podlegał zaskarżeniu lub, jeśli po ujawnieniu, inne firmy mogą legalnie wykorzystać ujawnione informacje dla uzyskania przewagi konkurencyjnej. Skutki ujawnienia należy dokładnie rozważyć przed złożeniem wniosku o ochronę patentową.

OCHRONA PATENTOWA W INNYCH JURYSDYKCJACH

Ochrona patentowa jest jurysdykcyjna. Ogólnie oznacza to, że patent ma prawne znaczenie w kraju, który go udzielił. Stany Zjednoczone są sygnatariuszem Konwencji paryskiej o ochronie własności przemysłowych, która ma około 160 sygnatariuszy. Konwencja paryska zasadniczo przyznaje roczny okres karencji na złożenie krajowych wniosków patentowych w każdym wybranym sygnatariuszu, aby uzyskać korzyść z pierwotnej daty zgłoszenia w Stanach Zjednoczonych. Alternatywą, dostępną dla członków konwencji paryskiej, jest ustawa o współpracy patentowej. Pozwala to na złożenie międzynarodowego patentu, który zasadniczo daje właścicielowi patentu 8–18-miesięczne okno na przetestowanie wykonalności, co upraszcza krajowy proces składania wniosków.

NARUSZENIE PRAW PATENTOWYCH

Podobnie jak środki zaradcze w przypadku naruszenia praw autorskich, środki zaradcze w przypadku naruszenia patentu obejmują środki zabezpieczające i odszkodowania, które zgodnie z ustawą nie są niższe niż rozsądna opłata licencyjna za naruszenie prawa. Jeśli naruszenie jest umyślne, szkody można potroić. Opłaty adwokackie mogą być przyznawane, ale tylko w wyjątkowych przypadkach. W obszarze eksportowanego oprogramowania komputerowego, kwestia noty pojawiła się w ramach 35 U.S.C. sekcja 271 (f). Sekcja 271 (f) została dodana w 1984 r. Do prawa patentowego, aby uniemożliwić naruszającym uniknięcie odpowiedzialności poprzez wykończenie towarów poza Stanami Zjednoczonymi. Osoba naruszająca prawo ponosi odpowiedzialność, jeżeli jej zamiarem jest wyprodukowanie lub dostarczenie elementu ze Stanów Zjednoczonych, który ma być połączony w innym miejscu, gdyby miało to miejsce, gdyby miało miejsce naruszenie w Stanach Zjednoczonych. Wyeksportowane oprogramowanie można uznać za „składnik" w sekcji 271 (f). W Microsoft Corp. przeciwko AT&T Corp. problem polegał na tym, czy dysk główny dostarczony przez Microsoft za granicą do powielania i instalacji za granicą swojego programu Windows narusza patent AT&T. Zastępując obwód federalny, Sąd Najwyższy stwierdził, że tak nie jest.

Sekcja 271 (f) zabrania dostaw komponentów „ze Stanów Zjednoczonych… w taki sposób, aby aktywnie wywoływać kombinację takich elementów". § 271 (f) (1). Zgodnie z tym sformułowaniem, same składniki dostarczone ze Stanów Zjednoczonych, a nie ich kopie, powodują § 271 (f) odpowiedzialność, gdy są łączone za granicą, aby utworzyć opatentowany wynalazek. Tutaj, jak zauważyliśmy, kopie Windows faktycznie zainstalowane na komputerach obcych nie były same dostarczane ze Stanów Zjednoczonych. W rzeczywistości kopie te nie istniały, dopóki nie zostały wygenerowane przez osoby trzecie poza Stanami Zjednoczonymi. Kopiowanie oprogramowania za granicą, wszystko może się

zgadzać, jest rzeczywiście łatwe i niedrogie. Ale to samo można powiedzieć o innych przedmiotach: „Klucze lub części maszyn mogą być kopiowane z mistrza; substancje chemiczne lub biologiczne mogą być tworzone przez rozmnażanie; a produkty papierowe mogą być wytwarzane za pomocą elektronicznego kopiowania i drukowania. ”… Brak jakichkolwiek przepisów dotyczących kopiowania w tekście ustawowym jest sprzeczny z orzeczeniem sądu, że powielanie za granicą kapitana wysyłanego ze Stanów Zjednoczonych„ dostarcza ”zagraniczne kopie z Stany Zjednoczone w ramach zmiany § 271 (f).

O ile nie zmieniono sekcji 271 (f), może to mieć poważne konsekwencje dla podważenia zdolności amerykańskiej firmy do kontrolowania naruszenia patentów, w przypadku gdy oprogramowanie jest elementem opatentowanego wynalazku.

PIRACTWO I INNE WTARGNIĘCIA

Tak długo, jak pomysły i innowacje były źródłem wartości handlowej lub społecznej, warunki, na których te pomysły i innowacje były dostępne do wykorzystania i wymiany przez innych, były przedmiotem znacznego napięcia. Chociaż wynalazcy i twórcy opłacalnych komercyjnie produktów i procesów chcą zmaksymalizować zwrot z inwestycji, presja rynku na efektywność kosztową (często motywowana chciwością ludzką i korporacyjną) napędza ciągłe dążenie do usunięcia opłat licencyjnych wynalazców i twórców z kosztów produkcja. Tak więc starożytne pojęcie piractwa, nieuprawnione wejście na pokład statku w celu kradzieży i nieuprawnione użycie innego wynalazku lub produkcji pozostaje żywe i dobre. Piractwo, o którym mówimy, nie jest po prostu nieautoryzowanym kopiowaniem milionów płyt kompaktowych (CD); w coraz większym stopniu obejmuje to nieautoryzowane usuwanie danych ze stron internetowych, nadużywanie autoryzowanego korzystania z Internetu, kradzież danych pracowników i podobne działania.

RYNEK

Zapotrzebowanie na nielicencjonowany dostęp do oprogramowania i multimediów oraz korzystanie z niego wzrasta rocznie. W ankiecie z 2017 r. Dotyczącej bezpieczeństwa komputerowego wśród instytucji korporacyjnych i rządowych, Instytut Bezpieczeństwa Komputerowego i Federalne Biuro Śledcze USA wykazały, że 59 procent wszystkich respondentów odkryło pracowników, którzy nadużyli przywilejów internetowych w różnych nieautoryzowanych celach. W badaniu przeprowadzonym w 2007 r. Przez stowarzyszenie Software & Industry Information Association zanotowano ogólnoświatowy spadek przychodów z piractwa (nielegalne kopiowanie i rozpowszechnianie) oprogramowania przekraczającego 28,8 mld USD w 2007 r. W krajach takich jak Chiny, przeciwnie, piractwo nie jest jedynie sankcjonowane, lecz stanowi inwestycję agencji rządowych. W ostatnich latach, w dużej mierze z powodu nasycenia dostępem do Internetu, nastąpiło ogromne rozpowszechnienie technologii mających na celu dostęp i dystrybucję (bez autoryzacji) chronionych aplikacji i mediów rozrywkowych. Stanowiło to ogromne wyzwanie dla posiadaczy licencji, ustawodawców i organów ścigania. Wyniki obejmowały próby ukarania zarówno nieautoryzowanego dostępu i wykorzystanie chronionego materiału. W tym procesie nastąpiła transformacja definicji tego, co jest chronione, oraz pewne zamieszanie co do zakresu tej ochrony, gdy w grę wchodzi Internet.

OCHRONA BAZ DANYCH

Bazy danych, uporządkowana kompilacja informacji w formacie elektronicznym, są istotnymi elementami każdej dyskusji o ochronie praw autorskich. Kompilacje informacji, danych i dzieł podlegają ochronie na podstawie ustawy o prawie autorskim. Aby zabezpieczyć ochronę praw autorskich do kompilacji, strona musi wykazać, że (1) posiadała ważne prawa autorskie do kompilacji; (2) domniemany sprawca naruszenia skopiował przynajmniej część kompilacji; oraz (3) część

skopiowana w ten sposób była chroniona zgodnie z ustawą o prawie autorskim. W tym kontekście ustawa o prawie autorskim chroni „oryginalny" wybór, koordynację lub układ danych zawartych w kompilacji. W zakresie, w jakim kompilacje zawierają informacje czysto faktyczne (np. Istniejące ceny produktów i usług), nie ma ochrony, ponieważ same fakty nie mają oryginalności. Nie ma znaczenia, że autor „stworzył" fakty dotyczące cen pobieranych za produkt lub usługę. Aby podtrzymać roszczenie dotyczące ochrony praw autorskich do kompilacji faktów, autor musi wykazać się kreatywnością w rozmieszczeniu danych. Standardowe lub rutynowe ustalenia są również poza parasolem aktu. Jest to sprzeczne z dyrektywą w sprawie bazy danych Unii Europejskiej, która nie wymaga kreatywności jako elementu ochrony bazy danych. Raczej chroni inwestycje w bazy danych pod ochroną praw autorskich, jednak pod względem kwalifikacji do dozwolonego użytku. Sąd Najwyższy Stanów Zjednoczonych orzekł, że kompilacja w bazie danych oryginalnych utworów autorów do gazet i czasopism narusza prawa autorskie poszczególnych autorów, gdy baza danych nie powiela artykułów autorów w ramach oryginalnego dzieła zbiorowego, do którego artykuły zostały wniesione. W New York Times Co., Inc. przeciwko Tasini, 105 autorów, którzy wnieśli artykuły i inne prace do New York Times, magazynu Time, i Newsday pozwali, gdy dowiedzieli się, że artykuły, które sprzedali wydawcom do wykorzystania w odpowiednich publikacje były reprodukowane i udostępniane online, za pośrednictwem LEXIS / NEXIS, internetowej bazy danych i na CD-ROM. W większości przypadków reprodukcje były pojedynczymi artykułami poza kontekstem gazety lub czasopisma, w zbiorze dzieł oddzielnie chronionych ustawą o prawach autorskich. Sąd Najwyższy uznał, że ponieważ wydawcy nowych utworów zbiorowych nie wnieśli oryginalnego lub twórczego wkładu do oryginalnych dzieł poszczególnych autorów, nie mogli reprodukować i rozpowszechniać tych utworów poza formatem, który każdy wydawca tworzył dla oryginalnych kolekcji dzieł , bez zgody lub płatności dla każdego autora.

ZASTOSOWANIE TRANSFORMACJI I DOZWOLONEGO UŻYTKU

Omówione wcześniej koncepcje wykorzystania transformacyjnego i dozwolonego użytku (w zakresie, w jakim można je oddzielić) odegrały znaczącą rolę w ostatnich decyzjach dotyczących autoryzowanego korzystania z mediów elektronicznych i Internetu. Punktem wyjścia dla tego zastosowania doktryny jest decyzja Sądu Najwyższego USA w Sony Corporation przeciwko Universal City Studios, Inc., słynnej bitwie o Betamax zainicjowanej przez przemysł filmowy. Chodziło o to, czy elektroniczne urządzenia rejestrujące mogą nagrywać programy telewizyjne, aby umożliwić osobom „czasowe" programy telewizyjne (tj. nagrywanie programów do oglądania w czasie innym niż czas nadawania). W swojej decyzji stwierdził sąd to przesunięcie czasowe było produktywnym wykorzystaniem programów telewizyjnych w celu innym niż pierwotna komercyjna transmisja i nie było próbą skopiowania pierwotnego celu ani wpłynięcia na rynek komercyjny tych programów. Trybunał podkreślił niekomercyjny element związany z przesunięciem czasu.

HOSTING INTERNETOWY I DYSTRYBUCJA PLIKÓW

Wzrostowi szerokości i zakresu Internetu towarzyszyły coraz większe pytania dotyczące zakresu, w jakim dystrybucja w inny sposób chronionych wyrażeń zmienia ich formę po konwersji na format elektroniczny. Pytania te pojawiają się w przypadku dostawców usług internetowych, którzy udostępniają ścieżkę dystrybucji chronionych materiałów oraz użytkowników końcowych, którzy publikują takie materiały na swoich stronach internetowych i tablicach ogłoszeń. Dla dostawców usług internetowych DMCA zapewnia pewien początkowy komfort. Tytuł II ustawy DMCA, oznaczony jako „Ustawa o ograniczeniu naruszania praw autorskich online", ustanawia kilka bezpiecznych portów dla dostawców usług w zakresie naruszenia praw. „Informacja znajdująca się w systemach lub sieciach w kierunku użytkowników" bezpieczna przystań jest dostępna dla każdego dostawcy „usług online lub dostępu do sieci, lub operatora ich urządzeń,. . . "W tym„ cyfrową komunikację online, między lub między punktami określonymi przez użytkownika, materiału wybranego przez użytkownika, bez

modyfikacji treści materiału wysłanego lub otrzymanego ”, który„ przyjął i wdrożył w rozsądny sposób oraz informuje subskrybentów i posiadaczy kont systemu lub sieci dostawcy usług, polityki, która przewiduje rozwiązanie w odpowiednich okolicznościach abonentów i posiadaczy rachunków systemu lub sieci dostawcy usług, którzy są sprawcami wielokrotnych naruszeń ”i„ dostosowuje się i nie koliduje ze standardowymi środkami technicznymi ”. kwalifikują się do bezpiecznej przystani, usługodawca musi wykazać, że:

1. Nie ma faktycznej lub konstruktywnej wiedzy, że informacje na temat jego systemu naruszają, nie jest świadomy okoliczności, z których naruszenie jest oczywiste, lub po uzyskaniu takiej wiedzy lub świadomości działa szybko, aby usunąć te materiały;

2. Nie otrzymuje żadnych korzyści finansowych bezpośrednio związanych z działalnością naruszającą, oraz

3. Po otrzymaniu zawiadomienia o naruszeniu materiałów w swoim systemie, odpowiada szybko, aby usunąć lub uniemożliwić dostęp do materiału.

Zakładając, że bezpieczna przystań nie ma zastosowania (na przykład, ponieważ dostawca usług internetowych nie działał na podstawie zawiadomienia o działalności naruszającej prawo), wielu usługodawców może jednak uniknąć odpowiedzialności. W pierwszym i przełomowym przypadku na ten temat, Centrum Technologii Religijnych przeciwko Netcom On-Line Communication Services, Inc., dostawca usług internetowych prowadził biuletyn usługa zarządu, na której publikacje Kościoła Scjentologii zostały opublikowane przez byłego ministra. Sąd Okręgowy stwierdził, że dostawca usług internetowych musi wykazać, że korzystanie z niego miało charakter pożytku publicznego (ułatwianie rozpowszechniania dzieł twórczych, w tym, ale nie wyłącznie, dzieła naruszającego prawo); że jego zysk finansowy nie był związany z działalnością naruszającą prawa (np. opłaty abonamentowe za dostarczanie systemów poczty elektronicznej zamiast opłat za wyświetlanie lub sprzedaż dzieła naruszającego prawo); że jego użycie nie było związane z wykorzystaniem właściciela dzieła; że dostawca usług internetowych skopiował tylko to, co było konieczne do świadczenia usługi; i że jego wykorzystanie materiału nie miało widocznego wpływu na potencjalny rynek pracy. W CoStar Group, Inc. przeciwko LoopNet, Inc. czwarty obwód opierał się na Netcom, jego kodyfikacji w DMCA, oraz na tym, że DMCA nie ogranicza stosowania innych środków ochrony przed naruszeniami i utrzymywał, że „automatyczne kopiowanie, przechowywanie i przesyłanie materiałów chronionych prawami autorskimi, gdy są one podsycane przez innych, nie powoduje ,że dostawca usług internetowych ściśle ponosi odpowiedzialność za naruszenie praw autorskich zgodnie z §§ 501 i 106 ustawy o prawie autorskim. ”Właściciele witryn internetowych i użytkownicy, którzy zamieszczają materiały rzekomo naruszające prawa, mają znacznie mniejsze trudności z odrzuceniem argumentów przemawiających za dozwolonym użytkowaniem. Było to szczególnie prawdziwe w warunkach czysto komercyjnych, gdy strona naruszająca prawa czerpie bezpośrednią korzyść finansową z materiału naruszającego prawa autorskie, a zamieszczony materiał jest dokładną kopią chronionego dzieła bez jakiejkolwiek transformacji na coś twórczego lub oryginalnego. W przypadku, który trafia do sedna natury otwartego dostępu do Internetu, jeden z sądów stwierdził niedawno, że właściciel praw autorskich, który publikuje swoją pracę w Internecie w celu bezpłatnej dystrybucji jako shareware, może pokonać transformacyjną obronę dozwolonego użytku, również publikując ekspresowe rezerwacja praw do dystrybucji

PRZESZUKIWACZE SIECI I DOZWOLONY UŻYTEK

Internet, oparty na otwartej wymianie danych i efektywności ekonomicznej, zrodził szereg narzędzi do wyszukiwania i agregowania danych, które skanują sieć w poszukiwaniu informacji żądanych przez użytkownika. Proces wykorzystywany przez te wyszukiwarki obejmuje identyfikowanie danych w sieci

Web, które są zgodne z parametrami wyszukiwania, a następnie pobieranie tych danych. Ponieważ kopiowanie zwykle odbywa się bez wyraźnej zgody właściciela praw autorskich, niektórzy twierdzą, że takie kopiowanie stanowi naruszenie. Chociaż istnieje bardzo mało precedensu dotyczącego stosowania transformacyjnego dozwolonego użytku w systemach automatycznego wyszukiwania danych, co najmniej jeden sąd utrzymał w mocy stosowanie obrony do roszczenia o naruszenie.

HYPERLINKING

W Perfect 10 v. Google, Inc., potwierdzone częściowo i zaniechane częściowo, Perfect 10, Inc. przeciwko Amazon.com, Inc. hostowane przez strony trzecie i strony internetowe P10, gdy wyszukiwarka obrazów Google wybrała je do wyświetlania w postaci pełnowymiarowych obrazów w ramkach oraz jako miniatury na komputerach i telefonach komórkowych. Sąd stwierdził, że hiperłącze nie stanowi wyświetlania w celu bezpośredniego naruszenia praw autorskich. W postępowaniu odwoławczym sprawa została przekazana do ponownego rozpatrzenia w celu ustalenia, czy postępowanie mieści się w ogólnej zasadzie odpowiedzialności składkowej. Aby docenić kontekst, w którym sądy zmagają się z tymi problemami w świetle nowych technologii, należy przeanalizować analizę Sądu Okręgowego.

UDOSTĘPNIANIE PLIKÓW

Transformacyjny dozwolony użytek nie ochroni pełnej retransmisji chronionej pracy na innym nośniku, gdy istnieje chronione dzieło o znacznym i szkodliwym wpływie na rynek. W A&M Records, Inc. przeciwko Napster, Inc. Napster umożliwił użytkownikom udostępnianie plików muzycznych przez Internet, pobierając oprogramowanie do udostępniania plików na dysk twardy, korzystając z oprogramowania do wyszukiwania plików muzycznych MP3 przechowywanych na innych komputerach, oraz przesyłanie kopii plików MP3 z innych komputerów. Sąd apelacyjny uznał, że użytkownicy Napstera jedynie retransmitowali oryginalne utwory na innym nośniku i że nie stanowiło to przekształcenia oryginalnego dzieła. Sąd uznał również, że udostępnianie plików muzycznych przez Internet miało i będzie miało znaczący i szkodliwy wpływ na istniejący i potencjalny rynek płyt CD i cyfrowych materiałów do pobrania dzieł właścicieli praw autorskich. W oparciu o nacisk Sony na rozróżnienie między użytkowaniem komercyjnym a osobistym, Sąd Apelacyjny stwierdził, że strona internetowa Napstera skutecznie udostępniła utwory do użytku publicznego, a nie tylko do osobistego użytku indywidualnych użytkowników. Upadek Napstera nie zakończył jednak kontrowersji związanych z udostępnianiem plików. Starając się uniknąć metody bezpośredniego udostępniania plików przez Napster, podmioty takie jak Grokster i StreamCast opracowały oprogramowanie do tworzenia sieci równorzędnych, za pomocą których poszczególne komputery komunikują się w celu wymiany plików bez konieczności centralnego serwera. Sąd Najwyższy niedawno ponownie rozważył naruszenie praw autorskich i udostępnianie plików w odniesieniu do tych sieci typu peer-to-peer i zastosował „zasadę wymuszania" do usług udostępniania plików. Dowody wykazały, że 90 procent plików dostępnych do pobrania z Grokster i StreamCast było dziełami chronionymi prawem autorskim, a Grokster i StreamCast przyznały, że większość użytkowników pobiera materiały chronione prawem autorskim. Istniało również mnóstwo dowodów na to, że dzięki swoim aplikacjom i reklamom oba podmioty sprzedawały się jako alternatywa dla Napstera, a ich modele biznesowe pokazywały, że „ich głównym obiektem [ive] było wykorzystanie ich oprogramowania do pobierania praw autorskich działa. "Sąd zwolnił sąd z apelacji potwierdzającej orzeczenie zbiorcze dla Grokster i StreamCast oraz odrzucił szeroką interpretację sądu odwołań od Sony Corp. przeciwko Universal City Studios, ale odmówił dalszego omówienia równowagi między ochroną dzieł chronionych prawem autorskim i promowanie handlu w kontekście tego, jak bardzo nieumiejętne korzystanie z każdej usługi było w stanie zapewnić, i wcale nie omawiała kwestii dozwolonego użytku. Zamiast tego Trybunał zauważył, że Sony nie wykluczyło innych form odpowiedzialności za naruszenie przepisów i, skupiając się na zamiarze

pozwanych w nakłanianiu do udostępniania plików, stwierdził, że „ten, kto dystrybuuje urządzenie w celu promowania jego wykorzystania w celu naruszenia praw autorskich, jak wynika z wyraźnego wyrażenia lub innych pozytywnych kroków podjętych w celu wspierania naruszeń, ponosi odpowiedzialność za wynikające z tego działania naruszenia przez osoby trzecie. ” Powołując się na Sony, Trybunał wyraził ponadto opinię, że zwykła znajomość potencjalnego lub rzeczywistego naruszenia nie jest wystarczającą podstawą do odpowiedzialności, ale że zasada ta stanowi… odpowiedzialność lokalu za celowe, zawinione wyrażenie i zachowanie, a zatem nie ma nic wspólnego z naruszeniem legalnego handlu lub zniechęcaniem do innowacji cel zgodny z prawem. ”Ponieważ usługa i oprogramowanie Grokster miały inne zgodne z prawem cele, decyzja Sądu Najwyższego podkreśla znaczenie udowodnienia zamiaru naruszenia lub spowodowania naruszenia. W związku z tym, zwracając się do sądu z wnioskiem o obejrzenie forteli i zrzeczeń, które ukrywają niezgodne z prawem cele, właściciel praw autorskich powinien rozważyć, jakie inne dowody istnieją lub mogą istnieć w zakresie projektowania produktu, reklamy, marketingu, komunikacji zewnętrznej i wewnętrznej, planów przychodów i innych czynników udowodniłoby to bezprawne zamiary. Ponadto, w przypadku właścicieli praw autorskich, problem pozostaje taki, że wielu dostawców oprogramowania do udostępniania plików może nie podlegać jurysdykcji sądów USA, a oprogramowanie do udostępniania plików, takie jak „Darknet”, zapewnia anonimowość użytkownikom nielegalnie pobierającym materiały chronione prawem autorskim. Jak zostanie omówione, wiele krajów jest sygnatariuszami TRIPS i subskrybuje międzynarodową ochronę praw autorskich. Po Grokster, producent oprogramowania do wymiany plików KaZaa został w Australii nakazany do używania swojego oprogramowania do popełniania naruszeń praw autorskich. Środek zaradczy wymagał zmiany oprogramowania, aby nie powielać dzieł chronionych prawem autorskim.

INNE NARZĘDZIA ZAPOBIEGAJĄCCE NIEAUTORYZOWANEMU WTARGNIĘCIU

Kilka zasad prawnych i przepisów wspiera prawo do zapobiegania i ścigania nieuprawnionych włamań. Obejmują one definicję wykroczenia, warunki użytkowania oraz kilka niezwykle ważnych i powszechnie stosowanych praw wyraźnie odnoszących się do problemów.

NARUSZENIE

Naruszenie to pojęcie prawa zwyczajowego, które wszyscy znamy, gdy stosuje się je do ziemi. Wszyscy widzieliśmy i prawdopodobnie w pewnym momencie naszej młodzieży naruszyliśmy znaki zakazu wkraczania, które są umieszczone na nieprzyjaznej własności sąsiada. Naruszenie to także koncepcja, która może dotyczyć komputerów i informacyjnych baz danych. Sądy przyjmują starsze koncepcje i ponownie stosują je w nowych sytuacjach. W eBay, Inc. przeciwko Bidder's Edge, Inc. Sąd Okręgowy przyznał eBay nakaz zabraniający Bidderowi korzystania z oprogramowania robota w celu zeskanowania informacji ze strony internetowej eBay. Sąd oparł nakaz na stwierdzeniu, że dostęp do strony internetowej w sposób, który wykracza poza zamieszczone w eBay zawiadomienie (były rzeczywiste listy sprzeciwu), stanowi naruszenie. Sąd uznał, że „sygnały elektroniczne wysyłane przez Bidder's Edge w celu uzyskania informacji z systemu komputerowego eBay [były] wystarczająco namacalne, aby wesprzeć wykroczenie powodujące działania”. Sąd ocenił również ciągłe naruszenie podstawowego prawa eBay do wykluczania innych osób z jego komputera system stwarzający wystarczającą nieodwracalną szkodę, aby uzasadnić nakaz. W związku z tym nie było konieczne, aby serwis eBay udowodnił, że dostęp rzeczywiście przeszkadzał w działaniu witryny. Przeciwnie, dowód „pośrednictwa lub korzystania z cudzej własności osobistej” był wystarczający, aby ustalić przyczynę działania na szkodę. Istotne jest to, że serwis eBay zezwalał innym osobom na dostęp do swojej strony internetowej na podstawie licencji, a sąd postrzegał postępowanie, które wykraczało poza licencjonowane użycie, po zawiadomieniu naruszającego, o naruszeniu praw autorskich. Jednak zastosowanie wykroczenia do nieautoryzowanej działalności komputerowej nie jest osiadłe. Tam,

gdzie wykroczenie dotyczy przedmiotu, a nie ziemi, musi istnieć nie tylko niewłaściwe użycie, ale także pewne szkody dla kondycji fizycznej lub wartości przedmiotu, lub niewłaściwe użycie musi pozbawić prawowitego właściciela korzystania z obiektu przez znaczny okres czas. Te dwa muszą być powiązane przyczynowo. W sprawie Intel przeciwko Hamidi Sąd Najwyższy w Kalifornii uchylił zakaz niższego sądu, który zakazał byłemu pracownikowi wysyłania niechcianych wiadomości e-mail z powodu naruszenia prawa. Sąd uznał, że zasięg doktryny został rozszerzony zbyt daleko, stwierdzając, że złe analogie (tj. Oglądanie serwerów jako domów i fal elektronicznych jako włamań) tworzą złe prawo. Sąd odmówił oglądania komputerów jako nieruchomości. Sąd, stwierdzając, że są one jak inne dobra osobiste, uznał, że komunikat ten nie różni się od listu dostarczonego pocztą lub telefonicznie. W skrócie, sąd odmówił znalezienia wykroczenia, ponieważ istniała „niepożądana komunikacja, elektroniczna lub inna", która fikcyjnie spowodowała „uszkodzenie systemu komunikacyjnego". biznes. Intel v. Hamidi po prostu przestrzega przed przekroczeniem zakresu stosowania pojęcia wykroczenia. Jeśli można wykazać uszkodzenie systemu komputerowego, pojęcie wykroczenia leży w arsenale środków zaradczych, zakładając, że intruz może zostać zidentyfikowany.

WARUNKI UŻYTKOWANIA

Warunki użytkowania mogą stanowić umowę dotyczącą korzystania ze strony internetowej. W związku z tym w każdej sytuacji, w której dostęp elektroniczny jest wymagany lub dozwolony, warunki użytkowania, wraz z potwierdzeniem, że takie warunki zostały zauważone i wyrażone na nie, mogą być egzekwowane jako ograniczenie użytkowania. W Register.com, Inc. v. Verio, Inc., Sąd Okręgowy utrzymywał wyrok nakazujący dostęp do strony internetowej głównie w kwestii umowy. Tam, jak opisał Sąd Okręgowy, pozwany Verio, przeciwko któremu wydano wstępny nakaz sądowy, był zaangażowany w działalność polegającą na sprzedaży różnorodnych usług projektowania, rozwoju i obsługi stron internetowych. W sprzedaży takich usług Verio konkurowało z działem tworzenia stron internetowych Register.com. Aby ułatwić sobie prowadzenie klientów, Verio zobowiązało się do codziennego uzyskiwania aktualizacji informacji WHOIS dotyczących nowo zarejestrowanych nazw domen. Aby to osiągnąć, Verio opracował zautomatyzowany program lub robota, który każdego dnia przesyłał wiele kolejnych zapytań WHOIS poprzez dostęp do portu 43 różnych rejestratorów. Po uzyskaniu informacji WHOIS o nowych rejestrujących Verio będzie wysyłać im oferty marketingowe za pośrednictwem poczty elektronicznej, telemarketingu i direct mail. W zakresie, w jakim prośby Verio zostały wysłane pocztą elektroniczną, praktyka była niezgodna z warunkami ograniczającej legendy Regostry.com dołączona do odpowiedzi na zapytania Verio. Najpierw zarejestrował się w Verio na temat tego zastosowania, a następnie przyjął nową restrykcyjną legendę na swojej stronie internetowej, która zobowiązała się do masowego namawiania „za pośrednictwem poczty bezpośredniej, poczty elektronicznej lub telefonicznie". Sąd uznał, że postępowanie Verio stanowiło umowę, taką jak kupowanie jabłek na przydrożnym stojaku na owoce, które Verio złamało:

Zdajemy sobie sprawę z tego, że oferty kontraktowe w Internecie często wymagają od użytkownika kliknięcia ikony „Zgadzam się". Bez wątpienia w wielu okolicznościach takie oświadczenie zgody oblężonego ma zasadnicze znaczenie dla zawarcia umowy. Ale nie we wszystkich okolicznościach. Podczas gdy nowy handel w Internecie naraził sądy na wiele nowych sytuacji, nie zmienił zasadniczo zasad umowy. Standardową doktryną umowy jest oferowanie świadczenia z zastrzeżeniem określonych warunków, a użytkownik podejmuje decyzję o skorzystaniu ze znajomości warunków oferty, przyjęcie oznacza akceptację warunków, które odpowiednio stają się wiążące dla oblata. („Milczenie i bezczynność działają jako akceptacja… gdzie użytkownicy czerpią korzyści z oferowanych usług z rozsądną możliwością ich odrzucenia i powodu, by wiedzieć, że były oferowane z oczekiwaniem odszkodowania").

* * *

Wracając do stoiska z jabłkami, gość, który widzi jabłka oferowane za 50 centów za sztukę i bierze jabłko, jest winien 50 centów, niezależnie od tego, czy powiedział, czy nie, „Zgadzam się". Wybór w takich okolicznościach polega na przyjęciu jabłko na znanych warunkach oferty lub nie braniu jabłka. Jak widzimy, oskarżony w Ticketmaster i Verio w tym przypadku miał podobny wybór. Każdy z nich miał dostęp do informacji podlegających warunkom, o których dobrze wiedział. Ich wybór polegał na zaakceptowaniu oferty kontraktu, przyjęciu informacji zgodnie z warunkami oferty lub, jeśli warunki były nie do przyjęcia, odmowie skorzystania z korzyści. Id., Na 403; a także był wykroczeniem, ponieważ:

Sąd okręgowy uznał, że użycie przez Verio [** 31] robotów wyszukujących, składających się z programów wykonujących wiele zautomatyzowanych kolejnych zapytań, pochłonęło znaczną część pojemności systemów komputerowych Register.com. Chociaż same roboty Verio nie obezwładniłyby systemów Registry.com, sąd uznał, że jeśli Verio uzyska dostęp do komputerów Registry.com za pośrednictwem takich robotów, „wysoce prawdopodobne" jest, że inni dostawcy usług internetowych opracują podobne programy, aby uzyskać dostęp do danych Registry.com, i że system zostanie przeciążony i ulegnie awarii. Nie możemy powiedzieć, że te ustalenia były nieuzasadnione. Id., Na 405. Podobnie, choć w innym ustawieniu, w ProCD v. Zeidenberg, gdzie ProCD sprzedało płytę CD z danymi nie do skopiowania. Dostęp do danych był jednak kontrolowany przez umowę licencyjną; jeśli nie było akceptacji, nie było dostępu. Umowa licencyjna zabraniała wykorzystywania danych do jakichkolwiek celów komercyjnych. Zeidenberg wziął dane i opublikował je na stronie internetowej, którą wykorzystywał komercyjnie do sprzedaży reklam. W ten sposób dane były wykorzystywane do przyciągnięcia odwiedzających. Sąd uznał, że ograniczenie licencji w zakresie użytkowania jest wykonalne. Znaczenie tej decyzji polega na tym, że tak długo, jak właściciel wyraźnie określa ograniczenia, ograniczenia mogą stać się umową, która jest akceptowana poprzez akceptację korzyści dostępu i może stanowić jedno zabezpieczenie przed nadużyciem dostępu.

USTAWA O OSZUSTWACH KOMPUTEROWYCH I NADUŻYCIACH

W 1984 r. Kongres przyjął oryginalną wersję ustawy o oszustwach komputerowych i nadużyciach (CFAA). Ogólnym celem była ochrona „komputerów interesu federalnego" poprzez kryminalizację celowego i nieautoryzowanego dostępu do komputerów, które spowodowały uszkodzenie komputerów lub przechowywanych na nich danych. Statut został znacząco zmieniony w 1986 r. I ponownie w 1996 r. I obecnie zawiera zarówno przepisy dotyczące egzekwowania prawa karnego, jak i prywatnego. Statut zakazuje tych działań:

… Świadomego uzyskiwania dostępu do komputera bez upoważnienia lub nadużywania uprawnień, a następnie uzyskiwania danych rządu USA, do których dostęp jest ograniczony i dostarczania lub próby dostarczenia danych osobie nieuprawnionej do ich otrzymania;

-celowy dostęp do komputera bez upoważnienia lub nadmiar uprawnień, a tym samym uzyskanie chronionych danych finansowych konsumentów;

-celowy i nieautoryzowany dostęp do komputera rządu USA, który wpływa na użytkowanie komputera przez rząd USA lub dla niego;

-dostęp do komputera wykorzystywanego w handlu międzystanowym świadomie i z zamiarem oszustwa oraz, w wyniku dostępu, oszukańczego uzyskania czegoś o wartości przekraczającej 5000 USD;

-spowodowanie szkód w komputerach używanych w handlu międzystanowym przez (i) świadome przesyłanie programu, kodu itp., który celowo powoduje takie szkody, lub (ii) celowy dostęp do komputera bez upoważnienia i powodując takie szkody;

-świadomie i z zamiarem oszustwa, handlu hasłami komputerowymi do komputerów używanych w handlu międzystanowym lub przez rząd USA; i

-przesyłanie zagrożeń powodujących uszkodzenie chronionego komputera z zamiarem wyłudzenia pieniędzy lub czegokolwiek wartościowego.

Punktem odniesienia pomiędzy odpowiednimi decyzjami dotyczącymi dostępu do danych w ramach CAFA jest to, czy dostęp jest „bez upoważnienia" czy „nadrzędny". Czynniki rozpatrywane przez sądy obejmują kroki podjęte przez właściciela informacji w celu ochrony przed ujawnieniem lub wykorzystanie, zakres wiedzy oskarżonych w zakresie ich uprawnienia do dostępu do danych i korzystania z nich, a także wykorzystanie danych po uzyskaniu dostępu. Historia legislacyjna wskazuje, że statut miał na celu „ukaranie tych, którzy nielegalnie wykorzystują komputery do celów komercyjnych". Ogólnie rzecz biorąc, istnieją dwa zestawy okoliczności do rozważenia. W pierwszej kolejności, czy rzeczywisty dostęp jest dozwolony, wyraźny czy dorozumiany? W kontekście internetowym, gdzie istnieje domniemanie otwartego dostępu, strona lub właściciele danych muszą wykazać, że podjęli kroki w celu ochrony zawartości swojej witryny i ograniczenia dostępu do danych, o których mowa. Po podjęciu tych kroków ochrona stanowi ścianę, przez którą nawet automatyczne systemy wyszukiwania nie mogą przejść bez wyraźnej zgody. Bez ściany muszą istnieć dowody na zamiar dostępu w niedozwolonym celu, jak wtedy, gdy Intuit wstawił pliki cookie do dysków twardych komputerów domowych. Po drugie, czy autoryzowany dostęp został nieprawidłowo przekroczony? Ogólnie rzecz biorąc, osoby, które korzystają z dozwolonego dostępu w nieautoryzowanym celu ze szkodą dla witryny lub właściciela danych, naruszyły CAFA. Przykładem mogą być pracownicy, którzy uzyskują informacje o tajemnicy handlowej i przekazują je za pośrednictwem systemu poczty e-mail pracodawcy do konkurenta, na który pracownik ma rozpocząć pracę; korzystanie z członkostwa w subskrypcji ISP w celu uzyskania dostępu do zbiorów adresów e-mail innych subskrybentów i ich zbierania w celu przesyłania niechcianych masowych wiadomości e-mail; oraz korzystanie z dostępu do systemu poczty e-mail pracodawcy w celu zmiany i usunięcia plików firmowych. Kary kryminalne wahają się od grzywien do pozbawienia wolności do 20 lat za wielokrotne przestępstwa. Jak omówiono później, umowa CAFA stała się znaczącym elementem roszczeń rządu USA i podmiotów prywatnych dążących do ochrony danych, które nie zawsze są chronione przez inne systemy ustawowe.

ZASTOSOWANIE DO INDEKSOWANIE STRON INTERNETOWYCH I BOTÓW

Roboty internetowe lub „boty" stały się powszechne, aby zebrać dane z witryn internetowych. Wszystkie te dane są ogólnie dostępne publicznie. Oznacza to, że każda osoba może uzyskać dostęp do tych samych informacji, ale nie z szybkością lub dokładnością przeglądarki internetowej. Ale kiedy takie „skrobanie" jest sprzeczne z CAFA? W jakim stopniu prawo chroni operatorów witryn lub dane firm przed przenikaniem przez zewnętrzną stronę trzecią? Kluczem do analizy w ramach CAFA jest pytanie, czy dane są faktycznie publicznie dostępne. Czy istnieją bariery techniczne, takie jak hasła lub kody, które należy obchodzić? Czy warunki użytkowania zabraniają dostępu lub użytkowania w inny sposób niż przez indywidualnego konsumenta? Pytania te mają zasadnicze znaczenie dla ustalenia, czy dostęp przekracza uprawnienia, czy nie ma uprawnień w ramach CAFA. Jeśli odpowiedź na którekolwiek z tych pytań (lub podobnych pytań) brzmi „tak", należy uważnie rozważyć dostęp, ponieważ taki dostęp i pobieranie danych prawdopodobnie narusza CAFA. W EF Cultural Travel v. Zefer Corporation Zefer zaprojektował bota do sieci Web, aby zeskrobać podróż i informacje o cenach z

witryny internetowej EF Cultural Travel (EF) do wykorzystania w konkurencyjnej witrynie travelWeb. Bot, zaprojektowany przez Zefera, pobierał informacje, dzwoniąc na adresy URL, na których przechowywane były poszczególne informacje o podróży i cenach, czytając kod źródłowy kluczowych funkcji i przechowując informacje w arkuszu kalkulacyjnym. Bot zrobił to w taki sposób, aby nie obciążać ani nie ingerować w stronę internetową EF. Po zebraniu informacje zostały przekazane konkurentowi, który wykorzystał te informacje do dostosowania oferowanej ceny i informacji o podróży. Skrobanie Zefera nie odbywało się w sposób ciągły, ale tylko w dwóch specjalnych przypadkach. EF pozwany, twierdząc, że nastąpiło naruszenie CAFA. Sąd Apelacyjny Pierwszego Okręgu nie zgodził się, odmawiając odczytania tego, co jest lub nie jest autoryzowane, standardem „rozsądnych oczekiwań", zamiast tego wymaga, aby operator strony internetowej wyraźnie określił ograniczenia dostępu w swoich warunkach. Po wydaniu wyroku w Federalnym Sądzie Rejonowym, Sąd Apelacyjny , wydał wyrok sumujący dla Zefera

PROSTE ŚRODKI ZAPOBIEGAWCZE

Nic dziwnego, że istnieje kilka metod zapobiegania nieuprawnionemu dostępowi w pierwszej kolejności i, jeśli nie powiedzie się, przeważają w późniejszych roszczeniach wynikających z CAFA. Być może najbardziej oczywistą miarą, którą podkreślił Pierwszy Sąd Apelacyjny, jest upewnienie się, że każdy odwiedzający witrynę jest odpowiednio poinformowany, że właściciel witryny zamierza jedynie ograniczać wykorzystanie lub dostęp do danych na stronie. Powiadomienie może przybierać różne formy. Na przykład wystarczający byłby wykrywalny komunikat, który można łatwo zidentyfikować na stronie głównej, ostrzegając użytkowników, że opublikowane informacje są dostępne tylko do oglądania, a nie do wykorzystania w jakikolwiek sposób niekorzystny dla zainteresowań gospodarza. Zrozumiałe jest, że większość hostów internetowych niechętnie publikuje takie rażące ograniczenia - niekoniecznie jest to „dobre dla biznesu". Dla osób zainteresowanych równie skuteczną, ale mniej bezpośrednią wiadomością, coraz powszechniejszą praktyką jest zmuszanie odwiedzających witrynę do rejestracji przed uzyskaniem dostępu do linków i innych stron dostępnych za pośrednictwem strony głównej. Im trudniejszy jest proces rejestracji, tym większy jest wyraźny zamiar gospodarza, aby ograniczyć dostęp do informacji, które będą dostępne po zakończeniu rejestracji. Gospodarze, którzy wymagają zapłaty pieniędzy, pewnego rodzaju członkostwa lub umowy o dostępie przed udzieleniem dostępu, ustalają, co dla celów ustaw, takich jak CAFA, które kryminalizują nieautoryzowany dostęp, będzie najczęściej postrzegane jako zapewniające wystarczające powiadomienie o granicach upoważnienia dostęp. W przypadku witryn członkowskich zakłada się, że każdy rejestrujący jest wstępnie kwalifikowany, a zatem upoważniony do przeglądania i wykorzystywania bardziej ograniczonych danych, przynajmniej do celów zgodnych z warunkami dostępu. Egzekwowalne umowy o dostępie do kliknięć ustanawiają nie tylko powiadomienie o ograniczeniach dostępu; zabezpieczają także zgodę każdego odwiedzającego na korzystanie ze strony internetowej i zawartych w niej danych w ramach podanych ograniczeń. Zabezpieczenie danych opartych na sieci Web przed nieautoryzowanym użyciem lub użytkownikami jest pod pewnymi względami sprzeczne z intencją i celem udostępniania informacji. W związku z tym jednak pytanie pojawiające się podczas publikowania informacji w sieci niewiele różni się od pytania zadawanego na przestrzeni wieków w zakresie, w jakim każdy z nas chce, aby nasi konkurenci lub przeciwnicy korzystali z naszej własności wbrew naszym interesom. Im większa troska, tym większe prawdopodobieństwo, że każdy host będzie musiał ograniczyć dane publikowane w sieci, lub zwiększyć świadomość każdego użytkownika na temat zasad dostępu.

KOMUNIKACJA ELEKTRONICNA I PRYWATNOŚĆ

Prywatność elektroniczna staje się problemem w naszym społeczeństwie baz danych i sieci. Większość amerykańskich statutów „prywatności" ma charakter przedmiotowy: Ustawa o telefonicznej ochronie

konsumentów z 1991 r. (Nie dzwoń, dla telemarketerów); Ustawa o odpowiedzialności za przenośność ubezpieczeń zdrowotnych z 1996 r. (Prywatność w odniesieniu do wykorzystywania i ujawniania informacji medycznych); Ustawa o ochronie prywatności dzieci w Internecie z 1998 r. (Regulująca zbieranie informacji od dzieci poniżej 13 roku życia przez strony internetowe skierowane do dzieci); Ustawa Gramm-Leach-Bliley z 1999 r. (Regulująca dzielenie się danymi klientów przez instytucje finansowe); Kontrolowanie napaści na nieprofesjonalną ustawę o pornografii i marketingu z 2003 r. (Ograniczanie spamerów i wymaganie możliwości rezygnacji); Fair and Accurate Credit Transaction Act z 2003 r. (zapewnienie bardzo ograniczonej pomocy w zakresie kradzieży tożsamości, takiej jak obowiązek dostarczenia rocznego raportu kredytowego). Przepisy te nie gwarantują prywatności w taki sam sposób, w jaki uczyniła to Unia Europejska w dyrektywie o ochronie danych z 1996 r. Dyrektywa UE w sprawie danych ustanawia ochronę przed udostępnianiem danych osobowych, w tym e-maili, w Unii Europejskiej, oraz ograniczenia w przekazywaniu takich danych poza UE do krajów lub firm, które nie posiadają równoważnych zabezpieczeń. W 2005 r. ChoicePoint, duży broker danych, przyznał, że sprzedał dane osobowe ponad 160 000 ludzi fałszywym firmom założonym przez złodziei tożsamości. Od tego czasu inne firmy ogłosiły włamania do danych i wycieki danych. W wyniku takich naruszeń bezpieczeństwa danych około połowa państw przyjęła przepisy, które wymagają ujawnienia nieuprawnionego dostępu do danych osobowych. W Stanach Zjednoczonych podstawową ochroną prywatności pozostaje pozew o torturowanie inwazji na prywatność. Ponieważ prawa te są określone przez państwo, przegląd wykracza poza zakres tego rozdziału. Jednak większość państw uznaje jakąś formę czynu niedozwolonego naruszania prywatności, a delikt został uznany w Restatement (Second) of Torts § 652, który to sąd odnosi się jako autorytatywne źródło prawa. Ogólnie rzecz biorąc, przekształcenie sprawia, że działania (a) celowe wtargnięcie, które jest wysoce obraźliwe dla rozsądnego człowieka, w odosobnienie cudzych spraw prywatnych, (b) publiczne ujawnienie prywatnych faktów, jeśli takie ujawnienie jest wysoce obraźliwe dla rozsądnej osoby, i nie jest uzasadnioną troską publiczną, oraz (c) przeznaczeniem na własny użytek lub na korzyść imienia lub podobieństwa innego. Tutaj już omówiono zobowiązanie powiernicze należne pracownikom swoim pracodawcom w odniesieniu do informacji poufnych. Rozwój deliktu prywatności sugeruje, że przedsiębiorstwa mają podobny obowiązek wobec swoich pracowników. Chociaż nieco inny zakres, ale zapowiadający rosnące prawo w tej dziedzinie, w Remsburg przeciwko Docusearch, Inc., Sąd Najwyższy w New Hampshire stanął przed firmą baz danych, która dostarczyła klientowi informacje, które zawierały dane osobowe kobiety . Klient użył jej, aby skonfrontować ją i zabić. Sąd Najwyższy w New Hampshire orzekł, że firma musiała działać „z należytą starannością w ujawnianiu danych osobowych osoby trzeciej klientowi". Decyzja ta jest jak dotąd bez odpowiedzi zaproszeniem do innych sądów. Na szczeblu federalnym CFAA oczywiście zajmuje się „nieautoryzowanym" dostępem do skomputeryzowanych informacji. Ponadto Kongres uchwalił pewne regulacje ustawowe, które w szczególności dotyczą komunikacji elektronicznej i prywatności.

WIRETAP ACT AND ELECTRONIC COMMUNICATIONS PRIVACY ACT

Ustawa o kontroli przestępczości i bezpiecznych ulicach z 1968 r., Ogólnie określana jako Federal Wiretap Act, ustanowiła ogólne parametry dozwolonego przechwytywania informacji przez organy ścigania. Zgodnie z pierwotnym założeniem, ustawa Wiretap obejmowała jedynie „komunikację przewodową i ustną". W 1986 r. Kongres uchwalił ustawę o ochronie prywatności w komunikacji elektronicznej (ECPA), która zmieniła ustawę Wiretap i stworzyła Stored Wire and Electronic Communications and Transactional Records Act (Stored Communications Act or SCA) aby „aktualizować i wyjaśniać federalne zasady ochrony prywatności i standardy w świetle zmian w komputerach i technologiach telekomunikacyjnych". SCA sprawia, że świadomie uzyskuje się dostęp do zabronionego obiektu usług łączności elektronicznej bez upoważnienia lub w nadmiarze, i za taki dostawca usług publicznych ujawnia informacje zawarte w takich obiektach. ECPA zezwala

prywatnemu powodowi na wniesienie roszczenia dotyczącego świadomego lub celowego naruszenia statutu w celu odzyskania rzeczywistych szkód lub ustawowego minimum 1000 USD. Nowelizacja z 1986 r. Rozszerzyła zakres ustawy Wiretap o „komunikację elektroniczną", która jest zdefiniowana jako „wszelkie przekazywanie znaków, sygnałów, pisania, obrazów, dźwięków, danych lub danych wywiadowczych o dowolnej naturze transmitowanych w całości lub w części przewodem, systemem radiowym, elektromagnetycznym, fotoelektronicznym lub fotooptycznym. „Intercept" definiuje się jako „fonetyczne lub inne pozyskiwanie treści dowolnej komunikacji przewodowej, elektronicznej lub ustnej za pomocą dowolnego urządzenia elektronicznego, mechanicznego lub innego. „W związku z tym ustawa Wiretap sprawia, że„ celowe przechwytywanie ... jakiejkolwiek komunikacji przewodowej, ustnej lub elektronicznej "jest przestępstwem". Definicje zawarte w ustawie obejmują teraz transmisje internetowe, takie jak wiadomości e-mail lub przesyłanie plików. Istnieje ważny wyjątek od tego zakazu. Zgodnie z wyjątkiem „zgody strony" dopuszczalne jest przechwytywanie komunikatów, w których „jedna ze stron komunikacji wyraziła uprzednią zgodę na takie przechwycenie". Wymagana zgoda może być wyraźna lub dorozumiana z okolicznych okoliczności. Ponadto pracodawca może uzyskać zgodę, informując pracownika o praktykach monitorowania w umowie o pracę lub w podręczniku pracownika. Zgodnie z „wyjątkiem dostawcy" dostawca usług łączności elektronicznej „którego udogodnienia są wykorzystywane do transmisji informacji przewodowej lub elektronicznej, [mogą] przechwytywać, ujawniać lub wykorzystywać tę komunikację w normalnym toku jego zatrudnienia podczas wykonywania jakiejkolwiek działalności jest to konieczny incydent… do ochrony praw lub własności dostawcy tej usługi. "Ten wyjątek może pozwolić pracodawcy na zgodne z prawem przechwytywanie komunikatów w celu wykrycia nieuprawnionego ujawnienia tajemnic handlowych osobom trzecim.

WSPÓŁCZESNE WYMAGANIA DOTYCZĄCE TRANSMISJI

Ustawa Wiretap zabrania jedynie przechwytywania łączności elektronicznej, termin, który został węziej zdefiniowany przez sądy niż sugeruje to definicja w akcie. Definicja przechwytywania zapewnia, że jednostka „przechwytuje" komunikację przewodową, ustną lub elektroniczną „tylko poprzez nabycie jej zawartości, niezależnie od tego, kiedy iw jakich okolicznościach ma miejsce nabycie". W kontekście tej sekcji powstaje poważne pytanie dotyczące legalność przechwytywania komunikacji elektronicznej w trakcie ich przesyłania i po ich zapisaniu, tymczasowo lub na stałe. Chociaż Kongres zamierzał zliberalizować swoją zdolność do monitorowania „komunikacji przewodowej", podczas gdy starał się sprawić, by sądy uznały, że Kongres zamierza uczynić nabywanie komunikacji elektronicznej niezgodnymi z prawem na mocy ustawy Wiretap „tylko wtedy, gdy nastąpią jednocześnie z ich transmisją" i zanim faktycznie przejdź przez linię mety i zapisz się. Jest to oczywiście interesująca fikcja w przypadku transmisji internetowych, które składają się z pakietów, które są rozbijane i przekazywane z routera do routera, a także z tymczasowej pamięci do tymczasowej pamięci. Jest to dalekie od przechwycenia rozmowy telefonicznej. Może być po prostu tak, że stosując język statutu, sądy stoją przed zastosowaniem go do technologii, która tak naprawdę nie istniała, gdy ustawa została zmieniona w 1986 r. W ostatnich latach sądy próbowały zastosować jednoczesną transmisję wymóg w różnych sytuacjach. Na przykład pliki cookie wykorzystywane do odzyskiwania danych osobowych odwiedzających witrynę internetową stanowią przechwycenie równoczesnej komunikacji elektronicznej i naruszenie ustawy Wiretap. Zauważając, że komunikacja elektroniczna odbywa się zazwyczaj w tranzycie i jest przechowywana jednocześnie, sąd uznał, że użytkownicy komunikowali się jednocześnie z siecią serwera klienta farmaceutycznego i serwer WWW firmy programistycznej, a zatem informacje zostały uzyskane jednocześnie z jego transmisją. Tam, gdzie transmisje elektroniczne znajdują się w pamięci RAM lub na dysku twardym, są one przechowywane w komunikacji i można je odzyskać, ponieważ znajdują się poza ustawą Wiretap. Podobnie wiadomość e-mail odzyskana po wysłaniu i odebraniu nie spełnia warunków jednoczesnej transmisji wymogu i dlatego nie został

przechwycony zgodnie z ustawą Wiretap. Być może w odpowiedzi na te i inne decyzje Kongres w 2001 r. Zmienił ustawę Wiretap, aby zastosować współczesny wymóg transmisji w celu połączenia komunikacji, której nie można było odzyskać, pozwalając tym samym na odzyskanie przechowywanej komunikacji przewodowej.

Konop przeciwko Hawaiian Airlines, Inc.

Decyzja Konop wydaje się być najczęściej cytowanym przypadkiem w kwestii „przechwytywania" na mocy ustawy Wiretap. Konop, powód, był pilotem linii lotniczych, który stworzył i prowadził stronę internetową, na której zamieszczał biuletyny krytyczne wobec swojego pracodawcy, Hawaiian Airlines, Inc. i związku lotniczego. Konop kontrolował dostęp do swojej strony internetowej, wymagając od odwiedzających zalogowania się przy użyciu nazwy użytkownika i hasła oraz poprzez utworzenie listy autoryzowanych użytkowników. Funkcjonariusz Hawaiian Airlines poprosił jednego z takich autoryzowanych użytkowników o pozwolenie na użycie jego nazwiska w celu uzyskania dostępu do strony internetowej. Oficer zalogował się kilka razy, a inny oficer, korzystając z tej samej techniki, również zalogował się, aby wyświetlić informacje zamieszczone w biuletynie Konopa. Konop w końcu złożył pozew przeciwko Hawaiian Airlines, twierdząc, że naruszył on ustawę Wiretap, gdy jej urzędnik uzyskał nieautoryzowany dostęp do strony internetowej Konop. Sąd po raz pierwszy powtórzył, że ustawa zabrania jedynie przechwytywania łączności elektronicznej. „Przechwycenie", jak stwierdził sąd, wymaga, aby strona nabyła informacje równoczesne z jej transmisją, a nie gdy znajduje się w pamięci elektronicznej. W tym przypadku sąd uznał, że pracodawca nie naruszył ustawy Wiretap, ponieważ funkcjonariusze uzyskali dostęp do komunikacji elektronicznej znajdującej się na stronie internetowej bezczynności, która nie spełniała wymogu jednoczesnej transmisji

STORED COMMUNICATIONS ACT.

W przeciwieństwie do ustawy Wiretap, The Stored Communications Act (SCA), jak sama nazwa wskazuje, ustanawia ograniczenia dostępu do przechowywanej komunikacji (tj. komunikacji dostępnej po ich przekazaniu). Specyficznie, SCA sprawia, że „umyślnie [dostęp] bez zezwolenia obiekt, przez który świadczona jest usługa komunikacji elektronicznej…, a tym samym [uzyskiwanie], [zmiana] lub [zapobieganie] autoryzowanemu dostępowi do drutu lub komunikacji elektronicznej, gdy jest on przechowywany w formie elektronicznej. "SCA definiuje„ elektroniczne przechowywanie "jako„ (A) dowolne tymczasowe, pośrednie przechowywanie drutu lub komunikacji elektronicznej związanej z elektroniczną transmisją; oraz (B) wszelkie przechowywanie takiej komunikacji przez dostawcę usług komunikacji elektronicznej w celu ochrony kopii zapasowej takiej komunikacji. "SCA zwalnia z odpowiedzialności„ uprawniony… przez osobę lub podmiot świadczący usługi łączności przewodowej lub elektronicznej "lub„ przez użytkownik tej usługi w odniesieniu do komunikacji lub przeznaczony dla tego użytkownika.

MAGAZYN ELEKTRONICZNY

<u>Pliki kopii zapasowych.</u>

Istotnym elementem, który oddziela SCA od ustawy Wiretap, jest to, że dostęp do komunikacji znajduje się w pamięci elektronicznej. Dlatego pierwsze pytanie dotyczy tego, co stanowi składowanie elektroniczne. W Theofel przeciwko Farey-Jones, Dziewiąty Sąd Apelacyjny USA próbował odpowiedzieć na to pytanie. Wezwanie do sądu wezwało dostawcę usług internetowych praktycznie do każdej wiadomości e-mail wysłanej lub otrzymanej przez ICA i jej pracowników. W odpowiedzi dostawca usług internetowych opublikował kilka wiadomości e-mail na stronie internetowej dostępnej dla Farey-Jonesa i jego prawników. Kiedy ICA dowiedział się o tych działaniach, pozwał Farey-Jonesa m.in. za naruszenie SCA. Według sądu w Theofel, Kongres uznał, że użytkownicy ISP mają uzasadniony

interes w ochronie poufności komunikacji w pamięci elektronicznej w ośrodku łączności. Ponadto tego uzasadnionego interesu nie można przezwyciężyć przez oszustwo lub przez kogoś, kto świadomie wykorzystuje błąd, który umożliwia dostęp do tego, co w inny sposób jest chronione. Sąd uznał, że użycie wezwania do sądu w celu uzyskania dostępu do e-maili ICA, gdy było dość jasne, przynajmniej w zakresie doradztwa, że wezwanie do sądu było nieważne, zanegowało wszelkie pozorne uprawnienia, które Farey-Jones i jego prawnicy mogli mieć na widok wiadomości e-mail ICA. Farey-Jones twierdził, że e-maile ICA nie znajdowały się w „magazynie elektronicznym" i dlatego nie doszło do naruszenia SCA. Sąd się nie zgodził. Jak wspomniano wcześniej, pamięć elektroniczna istnieje, gdy wiadomości są przechowywane tymczasowo, na podstawie pośredniej, jako część procesu przesyłania wiadomości do odbiorcy i gdy wiadomości są przechowywane jako część procesu tworzenia kopii zapasowej. W tym przypadku sąd stwierdził, że wiadomości e-mail, które najwyraźniej zostały dostarczone do ich odbiorców, były przechowywane przez dostawcę usług internetowych jako część procesu tworzenia kopii zapasowych w celu pobrania po pierwszym otrzymaniu. Dostęp do tych e-maili był zatem chroniony przez SCA, który naruszył Farey-Jones i jego prawnicy.

Tymczasowo przechowywana komunikacja.

Ostatnie przypadki interpretujące znaczenie „tymczasowego, pośredniego składowania… przypadkowego" transmisji przekazu były zgodne z literą prawa bardziej niż jego duchem. W dwóch przypadkach związanych z instalacją plików cookie, do których firmy programistyczne uzyskiwały dostęp w celach komercyjnych, sądy uznały, że pliki cookie są stale (lub przynajmniej na czas nieokreślony) instalowane na dysku twardym konsumenta i dlatego nie można ich uznać za „tymczasowe, pośrednie przechowywanie. „Decyzja Doubleclick podkreśliła również, że„ tymczasowy, pośredni element składowania SCA oznacza to, co mówi, to znaczy, że zakazane zachowanie obejmuje tylko nieuprawniony dostęp do komunikacji, gdy są tymczasowo przechowywane przez pośrednika i nie obejmuje dostępu do przechowywanych wiadomości po ich otrzymaniu. W kontekście prawa pracodawcy do zbadania wiadomości e-mail pracownika, pracownik nie będzie twierdził, że pracodawca naruszył SCA, gdy pracodawca otwiera e-maile wysłane lub otrzymane przez pracownika po otrzymaniu lub odrzuceniu wiadomości e-mail.

OPEN SOURCE

Wraz z ciągłym rozprzestrzenianiem się Internetu i oprogramowania komputerowego, licencjonowanie, dystrybucja i używanie otwartego kodu źródłowego zyskało rozgłos i zwiększyło znaczenie w praktyce własności intelektualnej i bezpieczeństwa komputerowego. „Open source" opisuje dystrybucję kodu komputerowego, który jest dostępny (tj. otwarty) dla wszystkich innych i dlatego umożliwia programistom komputerowym czytanie, stosowanie i modyfikowanie kodu, a także redystrybucję wszelkich zmian. Ruch open source rozpoczął się od Richarda Stallmana opracowanie Gnu's Not UNIX (GNU), darmowej formy UNIX-a, która miała być wolnym oprogramowaniem (za darmo w swobodzie używania, modyfikowania i dystrybucji oprogramowania). Rozwój GNU stworzył pierwszą licencję open source, General Licencja Publiczna (GPL). Linux, system operacyjny oparty na otwartym kodzie źródłowym i alternatywa dla Microsoft Windows, doświadczył ogromnego wzrostu dzięki wykorzystaniu licencji GPL. O powszechności kwestii open source świadczy formacja z 1998 roku inicjatywy Open Source Initiative (OSI), która nie tylko promuje rozwój open source i zachęca do korzystania z niego przez firmy, ale także oferuje łącza i informacje o większości dostępnych licencji open source.

LICENCJA OPEN SOURCE

Autor otwartego kodu źródłowego zawiera prawa autorskie, które działają tak, jak inne prawa autorskie, ale kod jest wydawany na podstawie określonej licencji na zasadzie innej niż własna. Istnieją

różne typy licencji open source. Pierwszą licencją open source była GPL, jak opisano. Oferuje najszersze zastosowanie wolnego oprogramowania. Natomiast inne licencje nie dążą do utrwalenia swobodnego charakteru konkretnego programu. Według Open Source Initiative, istnieje prawie 60 licencji open source dostępnych obecnie dla autorów kodu źródłowego, z których wszystkie potwierdzają pewne wymagania użytkownika oprogramowania.

GPL

Licencjonowanie na licencji GPL opiera się na idei „copyleft" Stallmana który zasadniczo wykorzystuje prawa autorskie jako narzędzie zapewniające ciągłą bezpłatną dystrybucję kodu źródłowego. Innymi słowy, GPL zapewnia prawa do aplikacji, modyfikacji i dystrybucji chronionego prawem autorskim kodu źródłowego tylko wtedy, gdy użytkownik zgadza się, że warunki dystrybucji pozostają takie same. Tworzy to niekończący się łańcuch licencji GPL dołączonych do przyszłych dystrybucji wersji oryginalnej lub pochodnej, niezależnie od ich formy. Ten niekończący się łańcuch często nazywany jest „efektem wirusowym" GPL, ponieważ kod chroniony przez GPL mnoży się z wszelkich modyfikacji oryginalnego kodu chronionego GPL. GPL dotyczy nie tylko oryginalnie chronionego oprogramowania, ale także tego, co ogólnie definiuje jako „Program":

Jakikolwiek taki program lub praca oraz „dzieło oparte na Programie" oznacza Program lub dowolną pracę pochodną na podstawie prawa autorskiego: to znaczy dzieło zawierające Program lub jego część, dosłownie lub z modyfikacje i / lub tłumaczenia na inny język.

Ponadto, chociaż GPL stanowi również, że niezależne i oddzielne sekcje pracy pochodnej nie podlegają warunkom GPL, gdy są dystrybuowane jako oddzielne prace, GPL ma zastosowanie, gdy użytkownik dystrybuuje te same niezależne i oddzielne „sekcje jako część całość, która opiera się na Programie.... "Szerokie zastosowanie programu do GPL dodatkowo wzmacnia efekt wirusowy licencji. Inne postanowienia GPL wymagają, aby użytkownicy rozpowszechniający dosłowne kopie kodu źródłowego publikowali powiadomienia o prawach autorskich, zrzeczenia się gwarancji i dostarczali kopie GPL. Ponadto modyfikator / użytkownik musi dołączyć do wszelkich modyfikacji powiadomienie o zmianie oprogramowania, musi bezpłatnie rozpowszechniać lub licencjonować oprogramowanie na rzecz osób trzecich oraz musi dostarczyć odpowiednie informacje o prawach autorskich, zrzeczenia się gwarancji i warunki GPL. Podsumowując, szerokie terminy GPL nie tylko dążą do osiągnięcia celów FSF w zakresie wolnego oprogramowania, ale także mają wpływ na to, czy autorzy wybrali GPL i czy firmy korzystają z oprogramowania objętego GPL.

INNE LICENCJE OPEN SOURCE

Licencja Berkeley Software Distribution (BSD) oraz licencja Massachusetts Institute of Technology (MIT) są bardzo podobne, ponieważ wymagają zarówno informacji o prawach autorskich, zrzeczeń gwarancji, jak i ograniczeń odpowiedzialności. BSD zabrania ponadto autorom lub podobnym organizacjom zatwierdzania programu, a także wymaga rozpowszechniania kopii warunków BSD z oprogramowaniem.

POLITYKI BIZNESOWE W ODNIESIENIU DO LICENCJI OPEN SOURCE

Kwestia, czy dystrybucja prawnie zastrzeżonej pracy, która zawiera niewielką część chronionych kodem GPL przedmiotów zastrzeżonych do warunków GPL, nigdy nie była przedmiotem sporu. Jest to jedno z zagrożeń związanych z używaniem oprogramowania open source. Kolejne ryzyko polega na tym, że nieprzestrzeganie warunków licencji GPL może prowadzić do postępowania sądowego. MySQL starał się nakłonić Progress Software Corporation do dystrybucji programu Gemini MySQL bez umowy zgodnej z GPL. Ponieważ istniał faktyczny spór co do tego, czy Gemini jest dziełem pochodnym lub

niezależną pracą na mocy licencji GPL, a ponieważ postęp przewidywał, że ujawni kod źródłowy Gemini i wycofał licencję użytkownika końcowego dla użytkowników komercyjnych, sąd nie wydał nakazu co do GPL. Biorąc pod uwagę rosnące wykorzystanie otwartego oprogramowania, firmy muszą opracować kompleksowe zasady dotyczące korzystania z otwartego oprogramowania, aby uniknąć odpowiedzialności i publicznie udostępniać własną, zastrzeżoną technologię. Obawy dotyczą zazwyczaj wymogów licencyjnych dotyczących dystrybucji oprogramowania i jego modyfikacji, ponieważ działania te zazwyczaj wymagają od firmy wydania kodu źródłowego dla każdej rozproszonej modyfikacji, a modyfikacje często kończą umowy wsparcia dostawców. Ponadto dystrybucja niezmodyfikowanego kodu źródłowego w ramach programu zastrzeżonego może wymagać od firmy wydania własnego, zastrzeżonego kodu źródłowego. Jest jednak bardziej prawdopodobne, że firma byłaby zobowiązana do rozpowszechniania otwartego oprogramowania lub musiałaby zapłacić odszkodowanie. Rozważania te należy rozwiązać nie tylko poprzez politykę firmy, ale także wybierając najlepszy kod źródłowy do wykorzystania w programowaniu, biorąc pod uwagę wewnętrzne i zewnętrzne potrzeby firmy oraz specyficzne wymagania licencyjne tego kodu źródłowego.

ZASTOSOWANIE MIĘDZYNARODOWE

Ponieważ prawa Stanów Zjednoczonych są prawem tylko jednego narodu wśród wielu, egzekwowanie prawa USA i ochrona praw własności intelektualnej w dużej mierze zależy od traktatów międzynarodowych. W zakresie, w jakim działania naruszające prawo lub piractwo mogą zostać uznane za występujące w Stanach Zjednoczonych lub osoby naruszające prawo można znaleźć w Stanach Zjednoczonych, wówczas Stany Zjednoczone mają wystarczającą jurysdykcję nad tymi aktami w celu egzekwowania swoich przepisów. Innymi słowy, takie podmioty mogą być pozywane bezpośrednio przed sądy Stanów Zjednoczonych za naruszenie prawa Stanów Zjednoczonych. Oprócz bezpośredniego egzekwowania ochrona międzynarodowa jest zwykle nośnikiem dwustronnych umów między Stanami Zjednoczonymi a poszczególnymi krajami lub funkcją międzynarodowych protokołów lub traktatów, których sygnatariuszem są Stany Zjednoczone. I tak na przykład Konwencja paryska o ochronie własności przemysłowej ustanawia system uznawania pierwszeństwa wynalazku, ale tylko wśród państw członkowskich. Ponadto istnieje Traktat o współpracy patentowej (PCT), wielostronny traktat z ponad 50 sygnatariuszami. PCT pozwala na złożenie wniosku międzynarodowego, który upraszcza proces składania wniosku, gdy patent jest poszukiwany w więcej niż jednym kraju. W celu ochrony praw autorskich istnieje również szereg międzynarodowych traktatów i umów, które obejmują konwencję berneńską, powszechną konwencję o prawie autorskim oraz porozumienie Światowej Organizacji Handlu (WTO). Umowa handlowa (NAFTA) w grudniu 1992 r. NAFTA odnosi się do własności intelektualnej i wymaga, aby państwa członkowskie zapewniały taką samą ochronę własności intelektualnej jak członkowie Układu ogólnego w sprawie taryf celnych i handlu (GATT). Co najmniej członkowie GATT muszą przyjąć cztery konwencje międzynarodowe, w tym konwencję paryską i konwencję berneńską. Te umowy, konwencje i traktaty w dużej mierze nie próbują pogodzić różnic w krajowych prawach własności intelektualnej. Poszczególne przepisy krajowe i niuanse są po prostu zbyt skomplikowane i istnieje zbyt wiele różnic w opiniach, aby oczekiwać, że różnice te zostaną wewnętrznie pogodzone. Raczej, w dużej mierze, te międzynarodowe porozumienia próbują skodyfikować wzajemność między państwami członkowskimi, tak aby każda uznała zasadność praw własności intelektualnej w drugim.

POROZUMIENIE W SPRAWIE HANDLOWYCH ASPEKTÓW PRAWA WŁASNOŚCI INTELEKTUALNEJ

W dniu 8 grudnia 1994 r. podpisano Porozumienie w sprawie handlowych aspektów praw własności intelektualnej (TRIPS). Podpisanie TRIPS wymagało wprowadzenia zmian w ustawach i przepisach Stanów Zjednoczonych w celu dostosowania ich do norm międzynarodowych. TRIPS był jednak produktem Stanów Zjednoczonych i innych krajów przemysłowych naciskających na silniejsze, bardziej

jednolite standardy traktatów międzynarodowych dotyczących własności intelektualnej. Podstawową strukturą TRIPS jest ustanowienie minimalnego standardu ochrony własności intelektualnej, przy czym każdy kraj członkowski może swobodnie przyjąć bardziej rygorystyczne normy. W rubryce stosowanej w Stanach Zjednoczonych TRIPS mają zastosowanie do praw autorskich, patentów, znaków towarowych, znaków usługowych, prac związanych z maską (projekty układów scalonych) i tajemnic handlowych. Obejmuje również oznaczenia geograficzne i wzory przemysłowe. Nie omówione przez TRIPS, choć część międzynarodowego żargonu własności intelektualnej, są prawa hodowców i wzory użytkowe. W związku z tym TRIPS nie ustanawia żadnych standardów odnoszących się do tych pojęć, pozostawiając ,że każdy naród powinien ustawić parametry ochrony niezakłócone przez TRIPS. Nie przypadkiem wynegocjowano TRIPS w kontekście GATT, który ustanowił międzynarodowe standardy taryf handlowych i zapewnił środki zaradcze w zakresie odwetu handlowego, gdyby takie normy nie były przestrzegane. Struktura GATT zapewniła środki, w ramach których kraje rozwijające się zgodziły się na obniżenie taryf handlowych w zamian za prawo do eksportu innowacyjnych produktów w ramach wyłącznego monopolu przenoszonego przez prawa własności intelektualnej. Drugą korzyścią wynikającą z formatu GATT było zapewnienie środków odwetowych w handlu, jeżeli zgodnie z postanowieniami TRIPS dotyczącymi rozstrzygania sporów WTO ustali, że istnieje niezgodność. W rzeczywistości jest oczywiste, że TRIPS przynoszą korzyści krajom przemysłowym, które są bardziej skłonne do przodowania w innowacjach i bardziej troszczą się o ochronę własności intelektualnej swoich obywateli. Główną koncesją wyrwaną przez kraje rozwijające się w ramach TRIPS było uzyskanie od 4 do 11 lat na wdrożenie TRIPS i dostosowanie ich krajowych przepisów do zgodności. TRIPS ogólnie odzwierciedla pogląd USA, który koncentruje się na podstawach ekonomicznych praw własności intelektualnej jako służących większym interesom społecznym. Istnieje zatem przejście od interesów „społecznych" do interesów „przedsiębiorstw". W szczególności TRIPS przyjmują wysokie minimalne standardy dla patentów, które będą wymagać znaczących zmian legislacyjnych w krajach rozwijających się. Sekcja dotycząca praw autorskich zapewnia jednak mniejszą ochronę niż może być zapewniona przez kraje europejskie, ale jest zgodna z leczeniem w Stanach Zjednoczonych. Krótko mówiąc, TRIPS odpowiada na obawy przedsiębiorstw w Stanach Zjednoczonych, że zbyt luźny system ochrony międzynarodowej umożliwił naśladowanie innowacji w Stanach Zjednoczonych poprzez kopiowanie i bezpośrednie piractwo.

TRIPS I TAJEMNICE HANDLOWE

W swojej kategorii „Ochrona nieujawnionych informacji" TRIPS zapewnia ochronę informacji, które są rutynowo określane jako tajemnice handlowe w Stanach Zjednoczonych. Państwa członkowskie są zobowiązane do wdrożenia przepisów, które chronią informacje posiadane zgodnie z prawem przed ujawnieniem, nabyciem lub wykorzystaniem przez inne osoby bez zgody i wbrew „uczciwym praktykom handlowym", jeżeli takie informacje są (a) tajemnicą, że nie są w domena publiczna, (b) ma wartość handlową, ponieważ jest tajemnicą, oraz (c) została poddana rozsądnym krokom w celu zachowania jej tajemnicy. Ponieważ dyskusje, które doprowadziły do TRIPS, nie są zachowane instytucjonalnie, w przeciwieństwie do Rekordu Kongresu Stanów Zjednoczonych, nie ma żadnej historii negocjacji, która mogłaby być konsultowana w celu wyjaśnienia znaczenia ustępów wprowadzających ochronę tajemnicy handlowej. Wydaje się jednak, że istnieją różnice w stosunku do całkowitej liczby zabezpieczeń zapewnionych w Stanach Zjednoczonych. Pojęcie domeny publicznej wyrażane przez TRIPS jest informacją, która „nie jest, jako ciało lub w precyzyjnej konfiguracji i montażu jego elementów, ogólnie znana lub łatwo dostępna dla osób w kręgach, które zwykle zajmują się rodzajem danych informacji . "Ten artykuł wydaje się dotyczyć technologicznych sformułowań informacji, w przeciwieństwie do ogólnych informacji handlowych, takich jak informacje finansowe, które są ogólnie uważane za zastrzeżone i poufne w Stanach Zjednoczonych. Skoncentrowanie się na formule technologicznej informacji chronionych jest wzmocnione wymogiem TRIPS, zgodnie z którym

informacje mają wartość handlową. W związku z tym inne rodzaje informacji, które nie są częścią przedmiotu obrotu, mogą być uznane za nie mające wartości handlowej i dlatego nie wchodzą w zakres ochrony. W zależności od konkretnej jurysdykcji w Stanach Zjednoczonych istnieje rozróżnienie między informacjami poufnymi a tajemnicami handlowymi na podstawie wymogu, aby tajemnica handlowa miała wartość handlową. To z kolei oznacza, że informacje, które nie są wykorzystywane komercyjnie, nie podlegają ochronie zgodnie z prawem tajemnicy handlowej. Na przykład wyniki nieudanych eksperymentów, które nigdy nie zaowocowały komercyjnym produktem, nie mają wartości handlowej, chociaż takie eksperymenty są z pewnością pomocne w następnej rundzie eksploracji, ponieważ są drogowskazami tego, czego nie robić. Wniosek, jaki należy wyciągnąć, jest taki, że nie należy zakładać symetrii zabezpieczeń tylko ze względu na przepis TRIPS. Zamiast tego, w ramach rozsądnych kroków w celu zachowania tajemnicy, przedsiębiorstwa muszą rozważyć starannie przemyślane i ustrukturyzowane postanowienia umowne, a także system buforowania danych, który pozostawia prawdziwie poufne dane w Stanach Zjednoczonych, nawet jeśli dostęp jest dozwolony na zewnątrz. Niewłaściwe pobieranie takich danych jest prawdopodobnie działaniami, które mają miejsce w Stanach Zjednoczonych, a takie czyny podlegają egzekwowaniu i karaniu zgodnie z prawem Stanów Zjednoczonych.

TRIPS I PRAWA AUTORSKIE

TRIPS obejmuje ogólny model ochrony praw autorskich w Stanach Zjednoczonych w swoim wstępnym oświadczeniu, że „[c] czysta ochrona obejmuje także wyrażenia, a nie idee, procedury, metody działania lub pojęcia matematyczne jako takie.” Wszystkie państwa członkowskie zgadzają się, że co do ochrona praw autorskich będzie miała zastosowanie konwencja berneńska. Zgodnie z konwencją berneńską czas trwania prawa autorskiego to życie autora plus 50 lat. Jeśli życie osoby fizycznej nie jest zaangażowane, wtedy zwykle upływa 50 lat od publikacji. Ponadto programy komputerowe, zarówno w kodzie źródłowym, jak i obiektowym, mają być chronione jako dzieła literackie na mocy konwencji berneńskiej. TRIPS uznaje również, że kompilacje danych mogą być chronione jako dzieła twórcze. Artykuł 10 paragraf 2 wyraźnie stanowi:

Kompilacje danych lub innych materiałów, zarówno w formie do odczytu maszynowego, jak i w innej formie, które z powodu wyboru lub uporządkowania ich zawartości stanowią wytwory intelektualne, będą chronione jako takie. Taka ochrona, która nie rozciąga się na same dane lub materiały, pozostaje bez uszczerbku dla jakichkolwiek praw autorskich do danych lub materiałów. (Dodano podkreślenie.)

Dlatego TRIPS ustanawiają pewne minimalne standardy w rosnącej debacie na temat tego, jakie zabezpieczenia będą miały bazę danych. W Stanach Zjednoczonych wyraźnym punktem rozgraniczającym dla niechronionych informacji są kompilacje, które reprezentują jedynie wysiłek „pocenie się w czoło”. Takie kompilacje nie mogą być chronione prawami autorskimi. Klasycznym przykładem wysiłku polegającego na poceniu się brwi jest kopiowanie i alfabetyczne porządkowanie nazwisk, adresów i numerów telefonów w książkach telefonicznych. W Stanach Zjednoczonych kluczem do ochrony praw autorskich jest oryginalny wkład twórcy w dobór i aranżację. Zatem zapewne przepis TRIPS naśladuje prawo Stanów Zjednoczonych. Unia Europejska (UE) obrała bardziej ochronną ścieżkę. W swojej europejskiej dyrektywie w sprawie bazy danych z 1996 r. Bazy danych EUGranted są chronione jako ich własna unikalna forma własności intelektualnej. Zgodnie z dyrektywą UE baza danych to „zbiór niezależnych utworów, danych lub innych materiałów uporządkowanych w sposób systematyczny lub metodyczny i indywidualnie dostępnych za pomocą środków elektronicznych lub innych”. Baza danych może być chroniona, ponieważ reprezentuje pracę „intelektualisty stworzenie ”lub dlatego, że zostało skompilowane poprzez„ znaczną inwestycję ”. Dyrektywa UE chroni takie bazy danych przed nieautoryzowanym wydobyciem lub wykorzystaniem przez okres 15 lat, z możliwością przedłużenia tego okresu o dodatkowe 15 lat, jeśli istniałby„ znaczący nowy inwestycja ”w bazie

danych. Taka ochrona obejmuje bazy danych członków UE oraz bazy danych obywateli innych krajów, które oferują zabezpieczenia podobne do UE. Stany Zjednoczone, pomimo szeregu wniosków legislacyjnych, nie przyjęły wspólnej zasady. Rezultatem, przynajmniej dla firm wielonarodowych, jest to, że podmioty, które polegają na bazach danych, powinny rozważyć „zlokalizowanie" takich baz danych w państwie członkowskim UE, aby skorzystać z ochrony bazy danych UE.

TRIPS I PATENTY

TRIPS wymaga, aby wszyscy członkowie uznali prawo do patentowania produktów lub procesów we wszystkich dziedzinach technologii. Wynalazek posiadający zdolność patentową musi być nowy, wynalazczy i mieć zastosowanie przemysłowe. Zgłoszenie patentowe musi w pełni i jasno ujawniać wynalazek, aby specjalista mógł przeprowadzić wynalazek. Należy również ujawnić najlepszy sposób realizacji wynalazku od daty zgłoszenia. Prawa patentowe mają być egzekwowane bez dyskryminacji ze względu na miejsce wynalazku lub czy produkt jest importowany lub produkowany lokalnie. Patent na produkt przenosi wyłączne prawo do zapobiegania, bez zgody wynalazcy, tworzenia, używania, oferowania do sprzedaży, sprzedaży lub importu produktu. Patent na proces przenosi wyłączne prawo do zapobiegania wszystkim powyższym produktom, które wynikają z procesu, jak również z samego procesu. Posiadacz patentu ma również prawo do przydzielania, przenoszenia lub licencjonowania patentu. Minimalny okres ochrony patentu wynosi 20 lat od zgłoszenia. TRIPS daje każdemu państwu członkowskiemu prawo do wyodrębnienia z patentowalności pewnych kwestii, których celem jest ochrona życia ludzi, zwierząt lub roślin, lub uniknięcie poważnego uszczerbku dla środowiska. Ponadto TRIPS zezwala państwu członkowskiemu na zezwolenie na inne wykorzystanie bez zezwolenia posiadacza patentu. Sekcja określająca, kiedy takie użycie jest dopuszczalne, jest najbardziej szczegółową sekcją wśród przepisów patentowych TRIPS. Zasadniczo zezwala na takie wykorzystanie tylko (a) po staraniach o uzyskanie licencji od posiadacza patentu na rozsądnych warunkach handlowych, (b) z odpowiednim wynagrodzeniem dla posiadacza patentu, (c) jeżeli takie użycie jest ograniczone głównie do rynek krajowy państwa członkowskiego, oraz (d) jeśli nastąpi przegląd decyzji zezwalającej, jak również rekompensaty, przez „wyższy organ w tym państwie członkowskim". Jedną z okoliczności przewidzianych przez TRIPS jest przyznanie drugi patent, którego nie można wykorzystać bez naruszenia wcześniejszego (pierwszego) patentu. W takich przypadkach państwo członkowskie może udzielić upoważnienia, jeśli wynalazek zawarty w drugim patencie stanowi „ważny postęp techniczny o znaczącym znaczeniu ekonomicznym" w odniesieniu do pierwszego wynalazku patentowego, a posiadaczowi licencji udzielonej na podstawie rozsądnych warunków udziela się licencji krzyżowej. pierwszy patent wykorzystujący drugi patent. W przypadku patentów procesowych TRIPS stwarzają ograniczone obciążenie domniemanego sprawcy naruszenia, aby udowodnić, że identyczny produkt został wyprodukowany przy użyciu innego procesu. W szczególności państwo członkowskie może założyć, że patent na proces został naruszony w okolicznościach, w których produkt jest nowy, lub gdy posiadacz patentu nie jest w stanie wykazać, jaki proces został faktycznie zastosowany

TRIPS I OGRANICZENIA ANTYKONKURENCYJNE

TRIPS uznaje, że niektóre praktyki licencyjne lub inne warunki dotyczące praw własności intelektualnej mogą ograniczać konkurencję, niekorzystnie wpływać na wymianę handlową i utrudniać transfer i rozpowszechnianie technologii. W związku z tym TRIPS zezwala państwom członkowskim na określenie praktyk, które stanowią nadużycie praw własności intelektualnej, oraz na przyjęcie środków kontroli lub ograniczenia takich praktyk, o ile rozporządzenie jest zgodne z innymi przepisami TRIPS. W przypadku, gdy obywatel państwa członkowskiego narusza prawa i przepisy innego członka dotyczące działań antykonkurencyjnych, TRIPS przewiduje prawo zaangażowanych narodów do poufnej wymiany informacji na temat obywateli i ich działalności.

ŚRODKI ZARADCZE I MECHANIZMY EGEZKWOWANIA.

Oczekuje się, że każdy kraj członkowski zapewni mechanizm egzekwowania na mocy swoich przepisów krajowych, aby umożliwić skuteczne działania przeciwko wszelkim aktom naruszenia. Takie procedury obejmują środki zaradcze zapobiegające aktom naruszenia, a także zapobiegające przyszłym aktom. TRIPS nakładają obowiązek, że wszystkie takie procedury są „sprawiedliwe i sprawiedliwe" i nie są „niepotrzebnie skomplikowane lub kosztowne" lub wiążą się z „nieuzasadnionymi opóźnieniami". Ogólnie rzecz biorąc, środki te oznaczają dostęp do cywilnych procedur sądowych z normami dowodowymi, które przenoszą ciężar do zgłaszającego naruszenie, gdy posiadacz praw przedstawi racjonalnie dostępne dowody na poparcie swojego roszczenia. Odszkodowania mogą zostać przyznane w wystarczającym stopniu, aby zrekompensować posiadaczowi praw naruszenie, jeśli „sprawca naruszenia wiedział lub miał uzasadnione podstawy, by wiedzieć, że angażuje się w działalność naruszającą prawa". Oznacza to, że czujność i zawiadomienie są niezbędne do zapewnienia znaczącej ochrony praw własności intelektualnej, ponieważ powiadomienie jest najlepszym sposobem na ustalenie roszczenia o odszkodowanie. TRIPS pozwala swoim członkom zezwolić na odzyskanie utraconych zysków lub z góry określonych (ustawowych) szkód, nawet jeśli sprawca naruszenia nie wiedział, że był zaangażowany w zachowanie naruszające prawo. Mimo że należy przewidzieć środki zabezpieczające, środki zaradcze mogą być ograniczone w okolicznościach dotyczących posiadaczy patentów, jak omówiono, w przypadku wypłacenia odpowiedniego odszkodowania, a domniemany sprawca naruszenia w inny sposób przestrzegał przepisów swojego prawa krajowego zezwalających na takie wykorzystanie po zapłaceniu rozsądnej rekompensaty . Aby zapobiec dalszemu naruszaniu przepisów, materiały naruszające prawo mogą być zamawiane jako zniszczone lub usuwane w celach komercyjnych. Oprócz środków cywilnych, TRIPS wymaga sankcji karnych w przypadku „umyślnego podrabiania znaku towarowego lub piractwa praw autorskich na skalę handlową".

ZMIANY W PRAWIE WŁASNOŚCI INTELEKTUALNEJ

AIA. „AIA to najważniejsza reforma patentów legislacyjnych od ponad 50 lat. AIA zmieni sposób przyznawania patentów, sposób postępowania sądowego w sprawach patentowych oraz rodzaje wynalazków, które mogą być przedmiotem patentów, między innymi. "Autor podsumował główne cechy AIA w szczegółowych dyskusjach dotyczących następujących obszarów:

* Zasada pierwszeństwa zgłoszeń stanowi teraz priorytet wynalazku

* Ustalono wcześniejszą obronę użytkownika komercyjnego

* Nowe postępowanie po przyznaniu grantu dotyczące wyzwań związanych z ważnością patentu

* Urząd Patentów i Znaków Towarowych (PTO) nie będzie już udzielał patentów na strategię podatkową

* Specjalny przegląd przejściowy dotyczący niektórych patentów związanych z produktami i usługami finansowymi

* Większość opłat PTO wzrośnie o 15 procent

* Dostępne będzie ograniczone badanie priorytetowe

* Nowe zasady będą miały wpływ na postępowanie sądowe ze strony podmiotów niepraktykujących

* Fałszywe zastrzeżenia dotyczące oznakowania są ograniczone

* Inne przepisy utrudnią atak na ważność patentów

Pełne informacje na temat przepisów są dostępne w bazie danych THOMAS Library of Congress

PROTECT IP ACT (PIPA).

Ustawa PROTECT IP Act (Zapobieganie rzeczywistym zagrożeniom internetowym dla kreatywności gospodarczej i kradzieży własności intelektualnej) lub PIPA, została wprowadzona w Senacie USA w maju 2011 r., Ale nie udało się jej dotrzeć do Senatu. Po szeroko zakrojonym sprzeciwie publicznym, w tym tymczasowym zaciemnieniu tysięcy stron internetowych w proteście przeciwko PIPA i ustawie o zatrzymaniu piractwa internetowego (SOPA, poniżej), ustawa została zawieszona w styczniu 2012 r. W oczekiwaniu na dalsze analizy. Główne punkty PIPA obejmują następujące elementy (cytując kilka sekcji z bazy danych THOMAS):

* Zapobieganie rzeczywistym zagrożeniom internetowym dla kreatywności gospodarczej i kradzieży ustawy o własności intelektualnej z 2011 r. Lub ustawy OCHRONA IP z 2011 r. (Ust. 3) Upoważnia prokuratora generalnego (AG) do rozpoczęcia: (1) osobistego działania przeciwko rejestrującemu niedomyślna nazwa domeny (NDN) używana przez stronę internetową poświęconą działaniom naruszającym prawa (ISDIA) lub właścicielowi lub operatorowi ISDIA dostępnego za pośrednictwem NDN; lub (2) jeśli takie osoby nie mogą zostać znalezione przez AG lub nie mają adresu w okręgu sądowym USA, akcja in rem (przeciwko samej nazwie domeny, zamiast takich osób) przeciwko NDN używanemu przez ISDIA.

* Definiuje ISDIA jako stronę, która: (1) nie ma znaczącego zastosowania innego niż angażowanie się lub ułatwianie naruszania praw autorskich, obchodzenie technologii kontrolujących dostęp do dzieł chronionych prawem autorskim, lub sprzedaż lub promowanie podrobionych towarów lub usług; lub (2) jest zaprojektowany, obsługiwany lub wprowadzany * Definiuje NDN jako nazwę domeny, dla której rejestr, który wydał nazwę domeny i obsługuje odpowiednią domenę najwyższego poziomu, oraz rejestrator nazwy domeny znajdują się poza Stanami Zjednoczonymi.

* Zezwala sądowi, na wniosek AG, po rozpoczęciu w ramach tej sekcji akcji związanej z NDN w trybie personam lub rem, aby wydać tymczasowy nakaz ograniczenia lub nakaz przeciwko NDN, rejestrującemu, właścicielowi lub operatorowi zaprzestania i zaprzestania dalszego postępowania Działalność ISDIA, jeśli NDN jest używany w Stanach Zjednoczonych w celu uzyskania dostępu do ISDIA kierującej działalność do rezydentów USA i wyrządzającej szkodę amerykańskim intelektualistom ,posiadaczom praw własności.

* Kieruje AG w celu zidentyfikowania i powiadomienia z wyprzedzeniem operatorów nieautorytatywnych serwerów systemu nazw domen (NDNSS), dostawców transakcji finansowych (FTP), internetowych usług reklamowych (IAS) oraz dostawców narzędzi lokalizacji informacji (ILT), w tym wyszukiwarek internetowych katalogi i inne indeksy z linkami hipertekstowymi lub odsyłaczami do lokalizacji online, których działanie może być wymagane, aby zapobiec takiej aktywności ISDIA związanej z NDN.

* Podaje środki zapobiegawcze, które muszą zostać podjęte przez NDNSS, FTPs, IAS i ILT po doręczeniu nakazu sądowego w takiej akcji związanej z NDN rozpoczętej przez AG.

* (Rozdział 4) Upoważnia AG lub właściciela praw własności intelektualnej poszkodowanych przez ISDIA do rozpoczęcia: (1) osobistej akcji przeciwko rejestrującemu nazwę domeny ISDIA lub właścicielowi lub operatorowi ISDIA, do którego dostęp uzyskuje się poprzez nazwę domeny; lub (2) jeśli takie osoby nie mogą zostać znalezione lub nie mają adresu w okręgu sądowym USA, akcja in rem przeciwko nazwie domeny używanej przez ISDIA.

* Zezwala sądowi, na wniosek właściwego powoda, po wszczęciu w ramach tego postępowania in personam lub in rem dotyczącego domeny, w celu wydania tymczasowego zakazu lub nakazu sądowego przeciwko nazwie domeny, rejestrującemu, właścicielowi lub operatorowi w celu zaprzestania i zaniechać dalszej działalności ISDIA, jeśli nazwa domeny jest: (1) zarejestrowana lub przypisana przez rejestratora nazw domen lub rejestr znajdujący się lub prowadzący działalność w Stanach Zjednoczonych, lub (2) używany w Stanach Zjednoczonych w celu uzyskania dostępu do ISDIA kierującego działalność do rezydentów USA i szkodzić posiadaczom praw własności intelektualnej w USA.

* Poleca właściwemu powodowi zidentyfikowanie i wcześniejsze powiadomienie FTP i IAS, których działania mogą być wymagane w celu zapobieżenia takiej działalności ISDIA.

* Wymaga, po doręczeniu mu nakazu sądowego po takiej in personam lub akcji naprawczej dotyczącej nazwy domeny, rozpoczętej przez AG lub właściciela prywatnego prawa na mocy niniejszej sekcji: (1) FTP do podjęcia uzasadnionych określonych środków zapobiegawczych, oraz (2)) MSR podejmują technicznie wykonalne i rozsądne środki.

* Ustanawia przepisy dotyczące podmiotów, które mogą być zobowiązane do podjęcia określonych środków zapobiegawczych w działaniach dotyczących zarówno nazw domen, jak i nazw NDN: (1) udzielenie immunitetu takim podmiotom za działania zgodne z nakazem sądowym, (2) upoważnienie właściwego powoda do wniesienia powództwo o wydanie nakazu sądowego przeciwko obsługiwanemu podmiotowi, który świadomie i umyślnie nie zastosuje się do nakazu sądowego, oraz (3) zezwalając takim podmiotom na interwencję w rozpoczęte działania i żądając modyfikacji, zawieszenia lub rozwiązania powiązanych nakazów sądowych.

* (Punkt 5) Zapewnia ochronę przed odpowiedzialnością za: (1) FTPs lub IAS, które w dobrej wierze dobrowolnie podejmują pewne działania zapobiegawcze przeciwko ISDIA oraz (2) rejestry nazw domen i rejestratorów, FTPs, ILT lub IAS, które w dobrej wierze, wstrzymaj usługi od stron naruszających prawo, które zagrażają zdrowiu publicznemu, rozpowszechniając leki na receptę, które są podrobione, zafałszowane, źle oznaczone lub bez ważnej recepty.

USTAWA O PIRACTWIE ONLINE (SOPA)

Stop Online Piracy Act (SOPA), H.R. 3261, podsumowano w bazie danych THOMAS w następujący sposób:

* … Upoważnia Prokuratora Generalnego (AG) do ubiegania się o nakaz sądowy skierowany przeciwko zagranicznej stronie internetowej kierowanej przez USA, która popełnia lub ułatwia piractwo internetowe, aby zażądać właściciela, operatora lub rejestrującego nazwę domeny lub samej witryny lub nazwy domeny, jeśli takie osoby nie są w stanie do znalezienia, do zaprzestania i zaniechania dalszych działań stanowiących określone przestępstwa własności intelektualnej w ramach federalnego kodeksu karnego, w tym do naruszenia praw autorskich, nieuprawnionego utrwalania i handlu nagraniami dźwiękowymi lub filmami z występów muzycznych na żywo, nagrywania wystawionych filmów lub handlu podróbkami etykiety, towary lub usługi.

* Ustanawia dodatkowy dwuetapowy proces, który pozwala posiadaczowi praw własności intelektualnej poszkodowanemu przez stronę kierowaną przez USA, poświęconą naruszeniom, lub stronie promowanej lub wykorzystywanej do naruszenia w określonych okolicznościach, aby najpierw dostarczyć pisemne powiadomienie identyfikujące witrynę do powiązanej płatności usługodawcy sieciowi i usługi reklamowe w Internecie wymagające od takich podmiotów przekazania powiadomienia i zawieszenia usług na taką zidentyfikowaną witrynę, chyba że właściciel, operator lub

rejestrujący nazwę domeny, po otrzymaniu przekazanego powiadomienia, dostarczy roszczenie wzajemne wyjaśniające, że nie jest dedykowane angażować się w określone naruszenia. Upoważnia uprawnionego do podjęcia działania w celu uzyskania ograniczonego nakazu sądowego przeciwko właścicielowi, operatorowi lub rejestrującemu nazwę domeny lub przeciwko samej witrynie lub nazwy domeny, jeśli takich osób nie można znaleźć, jeśli: (1) takie roszczenie wzajemne jest dostarczone (a jeśli jest to strona zagraniczna, obejmuje zgodę na jurysdykcję USA do rozstrzygnięcia, czy witryna jest poświęcona takim naruszenia) lub (2) dostawca sieci płatniczej lub internetowa usługa reklamowa nie zawiesza swoich usług w przypadku braku takiego roszczenia wzajemnego.

* Wymaga od dostawców usług internetowych, wyszukiwarek internetowych, dostawców sieci płatniczych i usług reklamy internetowej, po otrzymaniu kopii nakazu sądowego dotyczącego akcji AG, przeprowadzenia pewnych środków zapobiegawczych, w tym wstrzymania usług z witryny naruszającej prawo lub uniemożliwienia użytkownikom zlokalizowania Stany Zjednoczone od dostępu do strony naruszającej prawo. Wymaga od dostawców sieci płatniczych i internetowych usług reklamowych, po otrzymaniu kopii takiego zlecenia dotyczącego działania posiadacza praw, przeprowadzenia podobnych środków zapobiegawczych.

* Zapewnia odporność na odpowiedzialność dostawców usług, dostawców sieci płatniczych, internetowych usług reklamowych, reklamodawców, wyszukiwarek internetowych, rejestrów nazw domen lub rejestratorów nazw domen, którzy podejmują działania wymagane przez niniejszą ustawę lub w inny sposób dobrowolnie blokują dostęp lub kończą powiązanie finansowe z takimi witrynami .

* Zezwala takim podmiotom na zaprzestanie lub odmowę świadczenia usług na niektórych stronach, które zagrażają zdrowiu publicznemu poprzez dystrybucję leków na receptę, które są zafałszowane, niewłaściwie oznakowane lub bez ważnej recepty.

* Rozszerza przestępstwo naruszenia praw autorskich o publiczne występy: (1) dzieła chronionego prawem autorskim przez transmisję cyfrową oraz (2) prace przeznaczone do komercyjnego rozpowszechniania poprzez udostępnienie go w sieci komputerowej. Rozszerza przestępstwa związane z handlem towarami lub usługami z natury niebezpiecznymi, w tym: (1) podrabiane leki; oraz (2) towary lub usługi nieprawidłowo zidentyfikowane jako spełniające normy wojskowe lub przeznaczone do wykorzystania w bezpieczeństwie narodowym, egzekwowaniu prawa lub aplikacji infrastruktury krytycznej.

* Zwiększa kary za: (1) określone przestępstwa związane z tajemnicą handlową mające na celu przyniesienie korzyści obcemu rządowi, instrumentowi lub agentowi; oraz (2) różne inne przestępstwa związane z własnością intelektualną zmienione niniejszą ustawą.

* Nakazuje Komisji Wyrokowej USA, aby dokonała przeglądu iw razie potrzeby zmieniła powiązane federalne wytyczne dotyczące wydawania nakazów.

* Wymaga od sekretarza stanu i sekretarza handlu wyznaczenia co najmniej jednego załącznika własności intelektualnej, który zostanie przydzielony ambasadzie USA lub misji dyplomatycznej w kraju w każdym regionie geograficznym objętym biurem regionalnym Departamentu Stanu.

Krytycy ustawodawstwa to American Civil Liberties Association, niektórzy pedagodzy, niektórzy profesorowie prawa i United States Student Association. Argumenty obejmowały:

* Projekt ustawy doprowadziłby do usunięcia z Internetu znacznie nieuczciwych treści, co doprowadziłoby do naruszenia wolności słowa.

* Wyeliminowanie skupienia się w PIPA na koncentrowaniu się na witrynach poświęconych działalności naruszającej prawo zmarnowałoby zasoby rządowe na ogromną liczbę witryn.

* Dostawcy usług internetowych, operatorzy wyszukiwarek, dostawcy sieci płatniczych i usługi reklamowe będą musieli przestrzegać poleceń prokuratora generalnego, aby zablokować dostęp do stron zawierających treści naruszające prawa, blokując w ten sposób dostęp do wszystkich nie naruszających treści witryn.

* Zastosowania edukacyjne mogą być poważnie ograniczone, jeśli pojedynczy dokument naruszający prawo doprowadzi do zamknięcia całej witryny.

* Witryny z pojedynczym linkiem do treści naruszających prawa mogą zostać sklasyfikowane jako naruszenie „ułatwiające", a tym samym zostać zamknięte

* Rachunek naruszyłby standardy należytego procesu, pozwalając na administracyjne zamknięcie bez zapewnienia właścicielom oskarżonych stron możliwości obrony.

* Potencjalne bariery dostępu SOPA mogą poważnie wpłynąć na światowy ruch nacisku na dyktatorskie reżimy, takie jak w Chińskiej Republice Ludowej, w ich konsekwentnym tłumieniu swobodnego dostępu do informacji.

* Bibliotekarze, pedagodzy i studenci mogą podlegać zamknięciu administracyjnemu, nawet za to, co można uzasadnić uczciwym wykorzystaniem materiałów chronionych prawem autorskim.

Proponowany projekt ustawy został wycofany w tym samym czasie co PIPA

PATENTOWE TROLLE.

Grupy agresywnie atakujące użytkowników mało znanych patentów, często kupowane od wynalazców, którzy nigdy wcześniej nie korzystali ze swoich praw, są znane jako podmioty niepraktykujące lub trolle patentowe. Niektóre z tych firm poświęcają całą swoją działalność na pozywanie lub grożenie pozywaniem na podstawie nabytych patentów. W jednym znanym przypadku firma kupiła

„… Patent kanadyjski znany jako„ System wydawania automatycznych informacji, towarów i usług ", którego pełny tekst jest dostępny na stronie http://patents1.ic.gc.ca/ szczegóły? Numer patentu = 1236216 i język = EN CA [i] w szczególności adresy „System automatycznego wydawania informacji, towarów i usług klientowi na zasadzie samoobsługi, w tym centralne centrum przetwarzania danych, w którym przechowywane są informacje o usługach oferowanych przez różne instytucje w danej branży. Jedna lub więcej informacji samoobsługowych i terminale sprzedaży są połączone zdalnie z centralnym centrum przetwarzania danych i są zaprogramowane do gromadzenia informacji od potencjalnych klientów o pożądanych towarach i usługach, do przekazywania klientom informacji o pożądanych towarach lub usługach z centralnego centrum przetwarzania danych, do przyjmowania zamówień na towary lub usługi od klientów i przesyłanie ich do przetwarzania do centralnego centrum przetwarzania danych, akceptowanie płatności i dostarczanie towarów lub usług w FormularzU dokumentów do klienta po zakończeniu zamówień. Centralne centrum przetwarzania danych jest również zdalnie połączone z terminalami różnych instytucji obsługiwanych przez system, dzięki czemu każda instytucja może być aktualizowana na temat zakończonej sprzedaży usług oferowanych przez tę instytucję ".] Pomyśl o tym patencie. Czy nie przypomina ci to, co zrobiłeś ostatnio, kiedy zamówiłeś książkę lub kupiłeś coś w Internecie? Lub wykonałeś jakąkolwiek inną transakcję handlową w sieci?"

Badanie opublikowane przez Boston University School of Law230 wykazało, że trolle patentowe „… kosztowały amerykańskie oprogramowanie i sprzęt 29 miliardów USD w 2011 r.…" W Izbie Reprezentantów Peter DeFazio (D-OR) przedstawił HR.6245, Saving High -Tech Innovations from

Egregious Legal Disrupted Act z 2012 r., W sierpniu 2012 r. „zmieniłoby federalne prawo patentowe, aby umożliwić sądowi, po stwierdzeniu, że strona nie ma uzasadnionego prawdopodobieństwa powodzenia w postępowaniu kwestionującym ważność lub zarzut naruszenie sprzętu komputerowego lub patentu na oprogramowanie, przyznanie zwrotu kosztów postępowania sądowego stronie wygrywającej, w tym uzasadnione honoraria adwokackie.… ”.

W maju 2013 r. Senator Charles Schumer (D-NY) wprowadził S.866, ustawę o poprawie jakości patentów, poprawkę do AIA w celu przedłużenia jej przepisów dotyczących trudnych patentów na metody biznesowe. Baza danych biblioteki Kongresu THOMAS opisuje treść wniosku w następujący sposób:

* Zmienia ustawę Leahy-Smith America Invents Act w celu usunięcia ośmioletniego przepisu dotyczącego zachodu słońca w odniesieniu do przejściowego programu przeglądu po przyznaniu grantu dostępnego w celu przeglądu ważności patentów objętych metodą biznesową, dzięki czemu program jest stały.

* Rozszerza termin „patent na objęte metodą biznesową” o patent, który zastrzega metodę lub odpowiadające urządzenie do wykonywania przetwarzania danych lub innych operacji wykorzystywanych w praktyce, zarządzaniu lub zarządzaniu dowolnym przedsiębiorstwem, produktem lub usługą, z wyjątkiem wynalazków technologicznych. (Aktualne prawo ogranicza program do produktów lub usług finansowych).

UWAGI KOŃCOWE.

Bezpieczeństwo danych wiąże się ostatecznie z ochroną danych zastrzeżonych lub danych osobowych i własności intelektualnej. Konkurencja w zakresie legalnego nabywania i zatrzymywania własności intelektualnej jest niezmiennie zaspokajana przez nieetyczne i nielegalne wysiłki mające na celu pozbawienie prawowitych właścicieli ich praw. Konieczne jest zatem pełne poznanie mechanizmów i procedur wymaganych do ochrony tych praw jako części każdego komputera program bezpieczeństwa. Jednak wiele aspektów zjawisk prawnych pozostaje bez odpowiedzi lub zostało udzielonych odpowiedzi na ogół, a nie w kontekście konkretnego problemu. Roztropni strażnicy własności intelektualnej powinni stale monitorować odpowiednie ustalenia sądowe i być pewni, że zostaną zintegrowani w planowane podejście w celu ochrony tych najcenniejszych aktywów.