

ZNIKNĄĆ W SIECI – CZY TO MOŻLIWE? ANALIZA GRANIC ANONIMOWOŚCI

Kamil Ruszkowski
Uniwersytet Mikołaja Kopernika w Toruniu
Wydział Matematyki i Informatyki
ruszkowskik@mat.umk.pl

Abstract. Tools such as VPNs and private browsing mode are commonly perceived as allowing users to “disappear” on the internet. In practice, however, anonymity is not a binary attribute but a gradual property, dependent on the amount of information that can be used to identify an individual. Even among technically proficient users, anonymity is often misunderstood and its degree is significantly overestimated. This paper examines the limits of anonymity in the contemporary internet and argues why these boundaries are currently difficult to extend. Furthermore, it explores the trade-off between user anonymity and privacy on the one hand, and the convenience of everyday internet use and access to the services and benefits it offers on the other.

1. Wstęp

Postępujący wzrost roli internetu w życiu codziennym sprawił, że dane osobowe stały się towarem priorytetowym dla wielu podmiotów. Informacje dotyczące zachowań użytkowników, ich preferencji, lokalizacji czy aktywności w sieci są gromadzone, analizowane i wykorzystywane zarówno w celach komercyjnych, jak i politycznych. W krajobrazie opartym na algorytmach i danych, użytkownik stał się nie tylko konsumentem usług cyfrowych, lecz także źródłem cennych informacji, które mogą być przedmiotem obrotu, profilowania oraz zaawansowanej analizy.

Rosnąca wartość danych użytkowników powoduje również wzrost zagrożeń związanych z ich niewłaściwym wykorzystaniem. Zebrane informacje mogą zostać sprzedane podmiotom marketingowym, wykorzystane do budowy szczegółowych profili behawioralnych, albo sprawdzenia aktywności i preferencji pracowników na etapie rekrutacji, lub połączone z danymi pozyskanymi za pomocą technik Open Source Intelligence (OSINT) w celu identyfikacji konkretnej osoby [9][15]. W efekcie nawet użytkownicy przekonani o swojej anonimowości mogą zostać powiązani z określoną aktywnością internetową, poglądami czy historią wyszukiwania. Mogą także paść ofiarą

zjawisk takich jak doxxing (upublicznienie informacji personalnych w ramach zemsty bądź żartu), co niezwykle ma katastrofalne konsekwencje.

Próba ograniczenia tego rodzaju zagrożeń są regulacje prawne dotyczące ochrony prywatności i danych osobowych. Ich celem jest zapewnienie przejrzystości procesów przetwarzania danych oraz zwiększenie kontroli użytkowników nad informacjami na swój temat [1]. Niektóre rozwiązania legislacyjne mogą jednak prowadzić do skutków odwrotnych od zamierzonych. Przykładem jest brytyjska ustawa Online Safety Act, której założeniem była ochrona nieletnich przed szkodliwymi treściami, lecz która w praktyce doprowadziła do wprowadzenia mechanizmów weryfikacji tożsamości zwiększających ryzyko utraty anonimowości użytkowników [2]. Krytykę wzbudziły również propozycje regulacji znane jako Child Sexual Abuse Regulation (CSAR), wskazywane przez wielu badaczy jako potencjalne zagrożenie dla prywatności i bezpieczeństwa komunikacji elektronicznej, które jest zagrożeniem nie na poziomie poszczególniej jednostki, która może chcieć wykorzystać dane użytkowników, a na poziomie systemowym [13].

Oprócz danych osobowych i chęci rządów do weryfikacji tożsamości obywateli w internecie, zagrożeniem, szczególnie dla dzieci, są także social media. Współcześnie istniejące trendy i chęć bycia popularnym sprawia, że korporacje medialne nie muszą wcale zabiegać o to, aby najmłodszy udostępniali im jak najwięcej danych; pogoń za internetowymi trendami i potrzebą przynależności sprawia, że chętnie robią to same [11]. Związany z tym zagrożeniem dla anonimowości jest sharenting, czyli sytuacja, kiedy to rodzice publikują wrażliwe dane swoich dzieci [4].

Anonimowość w sieci jest zagrożona na wielu płaszczyznach. Wymienione wcześniej zagrożenia są zwykle skutkiem świadomej zgody użytkownika na korzystanie z konkretnej usługi, a ich skutki są redukowalne przy użyciu dobrych praktyk zwiększających anonimowość, ale istnieją także inne, mniej oczywiste nawet dla użytkownika, który stara się dbać o swój cyfrowy ślad. Największym i najczęściej spotykanym zagrożeniem dla anonimowości użytkowników są różnego rodzaju mechanizmy śledzące, ataki oraz socjotechniki, które zostaną rozwinięte w dalszych rozdziałach pracy.

2. OSINT i socjotechniki

OSINT to pozyskiwanie informacji o celu na podstawie dostępnych publicznie danych oraz analizy tych danych, aby uzyskać jak największą wiedzę o danej osobie, bądź mieć podstawy do pozyskiwania dalszych informacji. Źródłami takich danych mogą być social media, blogi, a nawet relacje z lokalnych portali informacyjnych. Dodatkową mocną stroną jest to, że aby deanonimizować internautów przy użyciu OSINTu nie jest potrzebna specjalistyczna wiedza o podatnościach usług, aplikacji, czy protokołów, ani znaczące umiejętności techniczne.

Szczególnie istotnym problemem jest możliwość korelacji pozornie nieistotnych fragmentów cyfrowego śladu w jeden spójny obraz. Techniki OSINT umożliwiają analizę nie tylko treści publikowanych przez użytkowników, ale również ich aktywności w czasie, interakcji społecznych oraz kontekstu wizualnego materiałów. W praktyce oznacza to, że nawet niewielkie ilości danych mogą zostać wykorzystane do identyfikacji osoby lub jej otoczenia. Zjawisko to jest dodatkowo wzmacniane przez trwałość danych w internecie — treści uznawane przez użytkowników za usunięte często pozostają dostępne w archiwach stron internetowych takich jak Web Archive. Ponadto istnieje gama narzędzi, które pozwalają na identyfikację kluczowych elementów tła na zdjęciach, aby odnaleźć dokładną lokalizację zrobienia zdjęcia (wyszukiwanie grafiką w Google, czy Yandex), rozpoznawanie twarzy i wyszukiwanie jej w innych miejscach w internecie (PimEyes), czy nawet rozpoznawanie szczytów górskich (PeakVisor).

Wystarczy jednak determinacja i podstawowa wiedza, aby nawet bez narzędzi zlokalizować dokładne miejsce zrobienia zdjęcia, ustalić czyjeś dane wrażliwe, lub miejsce zamieszkania. Przykładem tego jest działalność społeczności 4chana, która to przy użyciu analizy lotów samolotów w tle, konstelacji i wpisów z mediów społecznościowych była w stanie zlokalizować miejsce transmisji z akcji protestacyjnej aktywisty Shia La-Beoufa (transmisja odbywała się pośrodku pola, a jej jedynymi elementami były dźwięki otoczenia oraz widok flagi na tle nieba) i skutecznie przerwać tę akcję w zaledwie kilka dni [12]. Innym przykładem z tej samej społeczności jest udostępnienie lokalizacji bazy ISIS na podstawie elementów krajobrazu, małego budynku i słupów wysokiego napięcia widocznych w tle ich propagandowego filmu [17]. Ostatnim przykładem jest historia odkrycia i upublicznienia danych osobowych i miejsca zamieszkania osób znęcających się nad zwierzętami na podstawie filmiku wrzuconego przez te osoby do sieci [7].

Drugim istotnym elementem wpływającym na deanonimizację użytkowników są techniki socjotechniczne, które wykorzystują błędy ludzkie oraz podatności psychologiczne zamiast luk technicznych. Socjotechnika polega na manipulowaniu użytkownikiem w taki sposób, aby sam ujawnił informacje, które normalnie pozostałyby ukryte. Może to obejmować na przykład podszywanie się pod zaufaną instytucję, tworzenie fałszywego poczucia pilności lub wykorzystanie relacji interpersonalnych w celu zdobycia danych. Przykładem może być phishing, w którym atakujący tworzy fałszywą stronę logowania lub wiadomość e-mail, nakłaniając użytkownika do podania danych uwierzytelniających, lub, podszywając się pod bliską lub zaufaną osobę, prosi o dodatkowe dane osobowe, bądź informacje wrażliwe.

3. Mechanizmy identyfikacji użytkowników w sieci

Wbrew powszechnemu przekonaniu, identyfikacja użytkownika w internecie nie opiera się wyłącznie na adresie IP. Współcześnie, użytkownicy śledzeni są przez róż-

nego rodzaju mechanizmy śledzące, często niewidoczne lub nieunikalne w całkowitym stopniu.

Jednym z podstawowych źródeł informacji są metadane wymieniane podczas komunikacji pomiędzy przeglądarką a serwerem. Oprócz adresu IP obejmują one między innymi informacje o systemie operacyjnym, wersji przeglądarki, strefie czasowej, preferowanym języku czy konfiguracji urządzenia. Pojedynczo dane te rzadko pozwalają na jednoznaczną identyfikację użytkownika, jednak ich połączenie może znacząco zawęzić grupę potencjalnych osób korzystających z jakiegoś urządzenia [16].

Najbardziej rozpowszechnionym mechanizmem śledzenia pozostają pliki cookie. Są one wykorzystywane do przechowywania niewielkich ilości danych w przeglądarce użytkownika. Część z nich pełni funkcje niezbędne do działania witryny, takie jak utrzymywanie sesji logowania czy zapamiętywanie ustawień użytkownika. Znaczna część plików cookie służy jednak celom marketingowym. Dzięki nim podmioty reklamowe mogą rozpoznawać użytkownika podczas kolejnych wizyt oraz śledzić jego aktywność pomiędzy wieloma stronami internetowymi. W efekcie możliwe staje się tworzenie szczegółowych profili zainteresowań, preferencji zakupowych oraz zachowań online [5][18].

Fingerprint przeglądarki tworzony jest na podstawie szeregu parametrów technicznych, takich jak rozdzielczość ekranu, lista zainstalowanych czcionek, wersja systemu operacyjnego, konfiguracja sprzętowa czy dostępne rozszerzenia. Chociaż każda z tych informacji osobno występuje u milionów użytkowników, ich kombinacja często okazuje się wystarczająco charakterystyczna, aby odróżnić konkretną osobę od pozostałych internautów. Szczególnie zaawansowaną formą fingerprintingu jest canvas fingerprinting. Technika ta wykorzystuje różnice w sposobie renderowania grafiki przez poszczególne urządzenia i konfiguracje sprzętowo-programowe. Skrypt uruchamiany w przeglądarce generuje obraz przy użyciu elementu HTML5 Canvas, a następnie analizuje wynikowy układ pikseli. Niewielkie różnice wynikające z zastosowanego procesora graficznego, sterowników lub systemu operacyjnego pozwalają uzyskać charakterystyczny identyfikator urządzenia. Podobne podejście wykorzystywane jest w przypadku AudioContext fingerprintingu. W tej metodzie przeglądarka generuje określony sygnał dźwiękowy i analizuje sposób jego przetwarzania przez lokalny stos audio. Różnice pomiędzy urządzeniami, sterownikami oraz konfiguracjami systemowymi umożliwiają stworzenie kolejnego źródła informacji identyfikacyjnej [10][16].

Coraz większą rolę odgrywa również fingerprinting behawioralny. W przeciwieństwie do metod opartych na parametrach technicznych skupia się on na analizie zachowania użytkownika. Przedmiotem obserwacji mogą być np. godziny przeglądania, wyszukiwane frazy, zainteresowania, lub analiza stosowanego języka. Pozwala to na

precyzyjną identyfikację okresów aktywności, preferencji, lub bodźców, na które podatny jest cel, co, oprócz deanonimizacji, daje możliwości precyzyjnego dopasowywania reklam, lub ofert [3].

Dodatkowym źródłem danych są elementy osadzone przez podmioty trzecie. Widzety mediów społecznościowych, systemy analityczne oraz skrypty reklamowe są obecne na znacznej części współczesnych stron internetowych. Nawet jeśli użytkownik nie korzysta bezpośrednio z tych funkcji, samo załadowanie odpowiedniego skryptu może umożliwić przekazanie informacji o odwiedzonej witrynie do zewnętrznego podmiotu. Mechanizm ten pozwala na korelację aktywności użytkownika pomiędzy wieloma serwisami oraz stopniowe budowanie jego profilu [18].

Współczesne systemy śledzenia coraz częściej wykorzystują również korelację danych pochodzących z różnych źródeł. Informacje uzyskane z plików cookie, fingerprintingu oraz usług zewnętrznych mogą być łączone w celu zwiększenia skuteczności identyfikacji. Powoduje to, że nawet zastosowanie pojedynczych środków ochrony prywatności, takich jak usuwanie plików cookie czy zmiana adresu IP, często nie wystarcza do skutecznego ukrycia swojej aktywności w sieci. Dodatkowo rosnący trend wymuszania na użytkownikach założenie konta w serwisie i weryfikacja adresu email, bądź innych, istniejących kont, aby uzyskać dostęp do treści sprawia, że łączenie tych danych jest niezwykle proste.

4. Sieci anonimizujące

Sieci anonimizujące, szczególnie Tor, obrosły w wiele mitów, chociażby taki, że ich użytkownicy są nienamierzalni. Praktyka pokazuje, że jest to nieprawda; rozmaite specjalistyczne ataki deanonimizujące pozwalały na identyfikację nawet bardzo biegłych technicznie i świadomych użytkowników. Sieci te, tak jak „zwykły” internet, nie są również odporne na błędy wynikające z działalności użytkownika, takie jak podatność na socjotechniki, oversharing, czy błąd ludzki.

Tor, I2P, czy sieci miksujące pozwalają na znaczące zwiększenie stopnia anonimowości swoich użytkowników poprzez wiele rozbudowanych mechanizmów technicznych; takich jak onion routing, garlic routing, itp. Większość tych mechanizmów ukrywa ruch konkretnego użytkownika i w założeniu nie pozwala na identyfikację go poprzez routowanie wysyłanych przez niego pakietów przez wielu pośredników wybieranych całkowicie losowo. Każdy z wybranych pośredników pełni rolę proxy – tunelu, który ma jedynie umożliwić płynne przejście pakietu z jednego miejsca do drugiego. Proxy mają minimalną wiedzę o zawartości, celu, czy pochodzeniu pakietu przez wielokrotne warstwy szyfrowania, którymi obłożone są pakiety.

W sieci Tor komunikacja odbywa się poprzez onion routing; każdy pakiet, zanim dotrze do celu przechodzi przez trzy węzły (entry/guard, middle i exit). Węzeł wejściowy (entry) zna jedynie IP wysyłającego oraz następnego węzła, a cała reszta informacji

ukryta jest za warstwami kryptografii. Po dotarciu do węzła środkowego (middle) pakiet jest „obierany” z jednej z warstw kryptograficznych, a węzeł ten zna jedynie IP poprzedniego oraz następnego węzła. To samo „obranie” dzieje się na węźle wyjściowym (exit), a węzeł ten zna jedynie adres węzła środkowego i celu.

Oprócz tego, aby uniknąć identyfikacji pakietów, ich rozmiary są unifikowane do jednej, ustalonej wartości. Dodatkowym zabezpieczeniem jest unifikacja browser fingerprintu przeglądarki. Sporo elementów jest identycznych dla każdego z użytkowników Tora, co ogranicza możliwości ich rozróżnienia między sobą.

Dodatkowym elementem anonimowości są także onion services, czyli serwisy unikatowe dla sieci Tor, które wymagają znajomości konkretnego adresu .onion, aby uzyskać do nich dostęp. Tradycyjne wyszukiwarki nie pozwalają na odnalezienie ich przez to, że strony te nie są w żaden sposób indeksowane. Zgadnięcie takiego adresu również nie jest oczywiste, ponieważ wymaga odgadnięcia 56-znakowej kombinacji.

I2P z kolei ukrywa ruch również poprzez szukanie losowych ścieżek wśród węzłów, ale tutaj, zamiast świadomie hostowanych przez użytkowników węzłów, każdy komputer w sieci pełni taką rolę. Pakiety te przesyłane są z użyciem techniki garlic routing. Również okrywane są warstwami szyfrowania i również przy każdym odwiedzionym węźle jedna z warstw jest odkrywana, ale technika ta pozwala na spakowanie wielu pakietów do jednego (clove), gdzie każdy może podróżować do innego celu, inną ścieżką. Tak jak w przypadku Tora, wspierane są tutaj hidden services [8][18].

O ile to prawda, że sieci anonimizujące zapewniają dużo wyższy stopień anonimowości, tak również są one podatne na ataki deanonimizujące; wymagają jednak one dużo więcej czasu i środków.

Jednym z powszechnych typów ataków na takie sieci są ataki korelacyjne (correlation attacks), które polegają na analizie zależności pomiędzy ruchem wejściowym i wyjściowym z sieci anonimizującej. Nawet jeśli treść komunikacji pozostaje zaszyfrowana, obserwator może wykorzystywać cechy statystyczne transmisji, takie jak rozmiary pakietów, ich częstotliwość oraz ogólny wzorzec aktywności czasowej. Poprzez porównanie tych parametrów w różnych punktach sieci możliwe jest przypisanie ruchu wychodzącego do odpowiadającego mu ruchu wejściowego, co prowadzi do częściowej lub pełnej deanonimizacji użytkownika.

Kolejną istotną kategorią są ataki oparte na analizie czasowej (timing attacks), które wykorzystują zależności pomiędzy momentami wysyłania i odbierania pakietów. Nawet niewielkie opóźnienia w transmisji mogą tworzyć charakterystyczne wzorce, które przy odpowiednio dużej liczbie obserwacji mogą zostać wykorzystane do korelacji komunikacji na wejściu i wyjściu z sieci. W praktyce oznacza to, że anonimowość może zostać naruszona bez konieczności znajomości treści przesyłanych danych, wyłącznie na podstawie metadanych czasowych.

Ataki RAPTOR, z kolei, to ataki realizowane przez systemy autonomiczne (AS), które łączą trzy techniki zorientowane wokół protokołu BGP. Po pierwsze, wykorzystują one asymetryczną analizę ruchu – dzięki temu, że nagłówki TCP nie są szyfrowane na skrajnych końcach połączenia, napastnik może korelować numery sekwencyjne pakietów i potwierdzeń (ACK), obserwując ruch tylko w jednym kierunku u klienta i u serwera. Po drugie, atak wykorzystuje naturalną zmienność tras BGP (np. awarie łączy); każda zmiana ścieżki w czasie zwiększa szansę, że ruch w końcu przejdzie przez złośliwy AS, a do deanonimizacji wystarczy jednorazowa korelacja. Po trzecie, agresor może przeprowadzić aktywne porwanie BGP hijack lub BGP interception prefiksów IP węzła wejściowego, aby przejąć i przeanalizować ruch od komunikujących się z nim klientów, a następnie przesłać go dalej do celu [6][18][20].

Ostatecznie jednak, nawet najbardziej wyrafinowane technicznie zabezpieczenia sieciowe i kryptograficzne okazują się bezużyteczne w przypadku błędów użytkownika. Brak rygorystycznego odseparowania tożsamości wirtualnej od rzeczywistej prowadzi do natychmiastowej deanonimizacji. Najczęstszym przejawem tego zjawiska jest łączenie anonimowego przeglądania sieci z korzystaniem z social mediów, logowaniem się na swoje osobiste konta, czy oversharingiem.

Historia upadków administratorów największych rynków i serwisów w ukrytych sieciach dobitnie pokazuje ten mechanizm. Ross Ulbricht, twórca marketu Silk Road, zajmującego się handlem m.in. bronią i narkotykami, został zidentyfikowany, ponieważ na ogólnodostępnych forach programistycznych używał tego samego pseudonimu do promowania swojej platformy oraz do szukania pomocy technicznej, co na swoim markecie. Ponadto jako kontaktowy podał swój prywatny adres Gmail [14].

Podobne błędy popełnił również Lin Rui-Xiang, administrator Incognito Market. Powiązał on swoją tożsamość z nielegalnym rynkiem poprzez rozwijanie kodu zabezpieczającego giełdę na własnym, prywatnym i jawnym koncie GitHub, paniczne wyszukiwanie rozwiązań technicznych w czystym internecie po przejęciu serwerów przez służby, a także wielokrotne wykorzystywanie osobistego portfela kryptowalutowego do obsługi transakcji rynkowych [19]. Przykłady te dowodzą, że sieci anonimizujące są narzędziem wysoce warunkowym – ich techniczna skuteczność jest zawsze ograniczona ludzką dyscypliną. Ponadto trudność w obronie przed atakami deanonimizującymi sprawia, że anonimowość nie jest gwarantem, nawet w sieciach anonimizujących.

5. Dlaczego granice anonimowości są tak ciężkie do przesunięcia?

Powyższe rozdziały ukazują, jak trudne – lub wręcz niemożliwe – jest całkowite odcięcie się od mechanizmów zbierających dane. Przesunięcie granic anonimowości we współczesnym internecie napotyka na bariery, których natura nie jest wyłącznie technologiczna.

Rozwój internetu, a szczególnie social mediów spowodował, że dane osobowe, preferencje i inne dane o użytkownikach stały się towarem bardzo pożądanym, ponieważ stanowi to dla wielu firm cenne źródło wiedzy marketingowej. Ponadto rozwój możliwości i narzędzi do śledzenia aktywności lub identyfikacji na podstawie minimalnych informacji skutecznie utrudnia utrzymanie anonimowości przeciętnemu użytkownikowi.

Ostatecznie, granice anonimowości wyznacza sam człowiek, jego samodyscyplina i jego potrzeba interakcji społecznych. Internet przestał być jedynie narzędziem do biernego odbioru informacji, a stał się przestrzenią do budowania tożsamości. Pogoń za popularnością, potrzeba ekspresji w mediach społecznościowych, lub niewiedza, sprawiają, że użytkownik generuje zbyt duży i unikalny ślad cyfrowy. Ponadto, nawet przy używaniu najbardziej rozbudowanych technologii anonimizujących (takich jak sieci anonimizujące) wymagana jest bardzo duża uwaga i analizowanie każdej aktywności pod kątem potencjalnych zagrożeń pozwalających na identyfikację i wymusza na użytkowniku całkowite zrezygnowanie z rzeczy takich jak social media, czy zakupy online. Pełne „zniknięcie” w sieci oznacza więc często całkowite przestanie jej używania.

Literatura

1. A. M. Aseri, "The Implication of the European Union's General Data Protection-Regulation (GDPR) on the Global Data Privacy," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 4, pp. 692–702, Feb. 2020, [Online]. Available: https://www.researchgate.net/publication/344243565_The_Implication_of_the_European_Union%27s_General_Data_Protection_Regulation_GDPR_on_the_Global_Data_Privacy.
2. A. M. Azanya, "An Appraisal of the UK Online Safety Act 2023: Balancing Regulation, Rights, and Responsibilities," *ResearchGate*, Sep. 2025, [Online]. Available: https://www.researchgate.net/publication/395971015_An_Appraisal_of_the_UK_Online_Safety_Act_2023_Balancing_Regulation_Rights_and_Responsibilities.
3. C. Yang, Y. Zhu and N. Cheong, "Behavioral Fingerprints for User Identification via Unsupervised Matching, Supervised Learning of Data Augmentation, and Their Fusion," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 7, no. 4, pp. 597-609, Oct. 2025, doi: 10.1109/TBIOM.2025.3587435.
4. Doğan Keskin A., Kaytez N., Damar M., Elibol F., Aral N. Sharenting Syndrome: An Appropriate Use of Social Media? *Healthcare (Basel)*. 2023 May 9;11(10):1359. doi: 10.3390/healthcare11101359. PMID: 37239645; PMCID: PMC10218097.

5. E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, and E. P. Markatos, "User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users," in *Proceedings of the Web Conference 2021 (WWW '21)*, ACM, Apr. 2021, pp. 2130–2141, doi: 10.1145/3442381.3450056.
6. Evers, B., Hols, J., Kula, E., Schouten, J., den Toom, M., van der Laan, R. M., & Pouwelse, J. A. (2019). „Thirteen Years of Tor Attacks” Delft University of Technology [Online]. Available: <https://github.com/Attacks-on-Tor/Attacks-on-Tor>.
7. "Florida Girls Kill Rare Tortoise." [Online]. Available: <https://www.dailydot.com/un-click/florida-girls-kill-rare-tortoise>.
8. G. N. Tchabe and Y. Xu, "Anonymous Communications: A Survey on I2P," Technische Universität Darmstadt, Cryptography, Privacy and Security Group, Darmstadt, Germany, 2014. [Online]. Available: <https://i2p.net/docs/research/tchabe2014-anonymous-survey.pdf>.
9. H. M. N. Khan, M. S. Hosain, and H. Imam, "Pre-employment background check: Areview and research agenda," *Journal of Business Sectors*, vol. 2, no. 2, pp. 31–39, Oct.2024, doi: 10.62222/AXPC9543.
10. Hölbl, Marko & Zadorozhny, Vladimir & Družovec, Tatjana & Komapara, Marko & Nemeč Zlatolas, Lili. (2024). Browser Fingerprinting: Overview and Open Challenges. 10.3233/FAIA231163.
11. <https://www.eset.com/blog/en/home-topics/family-safety-online/kids-overshare-online-psychologist/>.
12. Internet Historian, "Capture the Flag | He Will Not Divide Us." [Online]. Available: <https://www.youtube.com/watch?v=vw9zyxm860Q>.
13. "Joint Statement of Scientists and Researchers on the EU's Proposed Child Sexual Abuse Regulation." [Online]. Available: <https://csa-scientist-open-letter.org/Sep2025>.
14. L. Gil Fersaca, "Ross Ulbricht and the Silk Road: A Cybercrime Investigation and ExpertWitness Guide," *SSRN Electronic Journal*, 2025, doi: 10.2139/ssrn.5507381.
15. M. Benjamin, "The Role of AI in Automating Employee Background Checks," Feb.2025, [Online]. Available: https://www.researchgate.net/publication/388687128_The_Role_of_AI_in_Automating_Employee_Background_Checks.
16. P. Laperdrix, B. Natarasanj, B. Baudry, and G. Avoine, "Browser fingerprinting: Asurvey," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–33, 2020.
17. Pezle, "The Time 4Chan Called in an Airstrike." [Online]. Available: https://www.youtube.com/watch?v=OR6epSP_Xlw.

18. Ruskowski K., "The Myth of the Anonymous User: A Study on Deanonymization on the Internet.", Feb.2026, doi: 10.13140/RG.2.2.21497.22883.
19. Y. Hoffman, "The Fall of a Dark Web Kingpin: Inside the Rise and Collapse of IncognitoMarket." [Online]. Available: <https://www.yanivhoffman.com/post/the-fall-of-a-dark-web-kingpin-inside-the-rise-and-collapse-of-incognito-market>.
20. Y. Sun, A. Edmundson, L. Vanbever, O. Li, J. Rexford, M. Chiang, and P. Mittal, "RAPTOR: Routing Attacks on Privacy in Tor," in Proceedings of the 24th USENIX Security Symposium (USENIX Security '15), Washington, D.C., USA, 2015. USENIX Association.