Jak jesteśmy profilowani w sieci?

Informacje o lekcji

Eksperci:	Wojciech Budzisz, Kamil Śliwowski, Michał „rysiek" Woźniak
Autorka wiedzy w pigułce:	Urszula Dobrzańska
Autorka scenariusza:	Weronika Paszewska
Organizacja publikująca:	Fundacja Panoptykon
Przedmiot:	Informatyka
Sugerowany poziom kształcenia:	Szkoły ponadgimnazjalne
Licencja:	Creative Commons Uznanie autorstwa – Na tych samych warunkach 3.0 Polska

Wiedza w pigułce

Korzystamy z różnych usług internetowych. Większość z nich wydaje się darmowa. Jednak to, że nie musimy wydawać pieniędzy, nie oznacza, iż nie ponosimy żadnych kosztów. Za wszystko płacimy swoimi danymi. Każda aktywność w sieci jest zapamiętywana i analizowana. Strony, z których korzystamy, nie tylko zachęcają do podawania wielu danych (np. przy tworzeniu konta), ale używają również ciasteczek (ang. *cookies*), czyli specjalnych plików zapisywanych na komputerach użytkowników. Część z nich jest niezbędna do tego, by prawidłowo wyświetlać stronę bądź umożliwić logowanie; wiele służy jednak do obserwowania tego, co robimy w Internecie. Do śledzenia naszej aktywności w sieci są wykorzystywane nie tylko ciasteczka.

Wiedza na temat naszych działań w sieci służy wielu podmiotom do różnych celów. E-marketerzy interesują się tym, z jakich korzystamy usług i produktów, by dopasowywać określone reklamy. Pracownicy banku, ubezpieczyciele czy potencjalny pracodawca przeglądają zawartość kont w portalu społecznościowym, by sprawdzić naszą wiarygodność. Państwo interesuje się tym, kto może stanowić zagrożenie dla bezpieczeństwa publicznego.

Każda osoba korzystająca z Internetu podlega profilowaniu. To mechanizm, który polega na kategoryzowaniu ludzi według cech i zachowań. Z profilowaniem spotkasz się np. na Facebooku, który zapamiętuje historię „lajków", by zaprezentować reklamę targetowaną, oraz w rozmaitych serwisach książkowych, filmowych czy muzycznych. Ich działanie opiera się na analizie decyzji użytkowniczek i użytkowników: zostaną Ci zaproponowane te tytuły, które wcześniej wybrały osoby sprofilowane jako podobne do Ciebie. Owszem, to bywa przydatne, ale zawsze ogranicza. Jeżeli na przykład ktoś korzysta z serwisu randkowego i zbytnio zaufa algorytmowi profilującemu, może stracić szansę na poznanie kogoś interesującego, ale całkowicie różniącego się od typowań systemu.

W zależności od tego, czy szukamy czegoś za pomocą szkolnego komputera, czy też swojego laptopa, otrzymujemy inne rezultaty. To dlatego, że znajdujemy się w tzw. bańce filtrującej (ang. *filter bubble*) – większość wyszukiwarek (np. Google, Bing) dopasowuje określone wyniki, bazując na historii zapytań. Ma to służyć wygodzie – i sprawdza się dobrze, gdy musimy szybko zlokalizować pobliską pizzerię, ale w wielu

sytuacjach może zawęzić zestaw odpowiedzi. Jeśli na przykład często szukasz w sieci informacji o wycieczkach zagranicznych, to po wpisaniu w wyszukiwarkę hasła „Turcja" możesz nie otrzymać ważnych informacji o odbywających się tam protestach. Będzie Ci również trudniej znaleźć opinie na dany temat, które – według systemów profilujących – różnią się od Twoich. To może zawęzić Twoje horyzonty.

Można niwelować negatywne skutki profilowania w sieci. Warto na przykład używać wyszukiwarek niewykorzystujących mechanizmu profilowania, a z Internetu korzystać po wylogowaniu z konta Google czy portali społecznościowych (więcej informacji w materiale pomocniczym „Jak się wydostać z bańki filtrującej").

Z profilowaniem spotkasz się nie tylko w sieci. Ludzie mogą być profilowani także przez państwo – i choć ma to miejsce w imię zwiększenia bezpieczeństwa, paradoksalnie bywa bardzo niebezpieczne. W USA na czarną listę pasażerów trafiają małe dzieci, które nazywają się tak samo lub podobnie jak osoby podejrzane o popełnienie przestępstwa. Nie mamy żadnego wpływu na interpretację informacji na nasz temat – w Wielkiej Brytanii organy ścigania oznaczały pasażerów linii lotniczych zamawiających wegetariański posiłek (!) jako osoby, które w przyszłości mogą zagrozić bezpieczeństwu państwa.

Skoro przy profilowaniu pomylić się może policja bądź inne służby – to tym bardziej wyszukiwarka internetowa.

Pomysł na lekcję

Zajęcia przybliżają temat profilowania w sieci. Przedstawione zostanie pojęcie bańki filtrującej. Uczestnicy i uczestniczki zastanowią się nad konsekwencjami profilowania w sieci oraz nad tym, jakie działania ograniczające profilowanie są w stanie podjąć.

Cele operacyjne

Uczestnicy i uczestniczki:

- znają pojęcie bańki filtrującej;
- wiedzą, kto i jakimi informacjami o nich może być zainteresowany;
- potrafią podać przykładowe konsekwencje profilowania użytkowników w sieci;
- znają sposoby, dzięki którym mogą ograniczać efekty profilowania.

Przebieg zajęć

Ćwiczenie 1.

Czas: *15 min*

Metoda: *miniwykład osoby prowadzącej, rozmowa*

Pomoce: *tablica i kreda, Wiedza w pigułce, Słowniczek*

Na podstawie Wiedzy w pigułce i Słowniczka opowiedz o bańce filtrującej. Zwróć uwagę przede wszystkim na:

- wyjaśnienie, czym jest bańka filtrująca;

- poinformowanie, kto czerpie korzyści z profilowania użytkowników w sieci;
- zaznaczenie, że użytkownicy są profilowani na podstawie ich aktywności w sieci.

Następnie zapytaj uczestników i uczestniczki, na podstawie jakiej aktywności w sieci następuje profilowanie. Pojawiające się odpowiedzi zapisuj na tablicy w formie mapy myśli. Jeśli się nie pojawią, zwróć uwagę na:

- słowa wpisywane w wyszukiwarkę,
- informacje ujawniane w sieci (płeć, wiek),
- „polubione" strony w serwisach społecznościowym,
- treść e-maili,
- odwiedzane strony internetowe,
- oglądane i kupowane przedmioty w sklepach internetowych,
- zainstalowaną przeglądarkę internetową,
- geolokalizację,
- ustawienia językowe.

Ćwiczenie 2.

Czas: *20 min*

Metoda: *praca w grupie, prezentacja*

Pomoce: *długopisy, karta pracy dla grup „Konsekwencje profilowania"*

Podziel uczestników i uczestniczki na grupy 4-osobowe. Rozdaj każdej grupie kartę pracy dla grup „Konsekwencje profilowania". Poproś grupy o zapoznanie się z instrukcją i rozwiązanie zadania. Następnie poproś grupy o prezentację rozwiązania jednej historii.

Odpowiedzi, które mogą się pojawić, to:

- wyższa cena usługi;
- zawężone wyniki wyszukiwania dostosowane do zainteresowań;
- ujawnienie informacji, które chcemy zachować dla siebie;
- utrata kontroli nad informacjami.

Ćwiczenie 3.

Czas: *10 min*

Metoda: *praca w parach, rozmowa*

Pomoce: *wydrukowany i pocięty materiał pomocniczy „Jak się wydostać z bańki filtrującej"*

Poproś uczestników i uczestniczki, żeby dobrali się w pary. Rozdaj każdej parze materiał pomocniczy „Jak się wydostać z bańki filtrującej". Poproś pary, żeby zapoznały się z działaniami i zastanowiły się, które są dla nich łatwe, a które trudne do realizacji i z jakiego powodu (w razie potrzeby wyjaśnij, że Chromium jest otwartym projektem przeglądarki internetowej, różnym od Google Chrome).

Na koniec zapytaj uczestników i uczestniczki, co było dla nich nowe i ciekawe, czego się dowiedzieli. Możesz również zapytać, które rozwiązania będą stosować, a które nie i z jakiego powodu. Zapytaj, kogo mogą poprosić o pomoc, jeśli będą mieli trudność z wdrożeniem któregoś z pomysłów. Zachęć ich do wzajemnego dzielenia się wiedzą.

Ewaluacja

Czy uczestnicy i uczestniczki po przeprowadzonych zajęciach:

- znają pojęcie bańki filtrującej?
- wiedzą, kto i jakimi informacjami na ich temat może być zainteresowany?
- potrafią podać przykładowe konsekwencje profilowania użytkowników w sieci?
- znają sposoby, dzięki którym mogą ograniczać efekty profilowania?

Opcje dodatkowe

Ćwiczenie 2 możesz rozwinąć. Po omówieniu odpowiedzi poproś grupy o wymyślenie takich wersji historii, w których użytkownicy i użytkowniczki nie są profilowani. Poproś grupy o wypisanie w punktach, co będzie odróżniać te 2 sytuacje.

Materiały

- Karta pracy dla grup „Konsekwencje profilowania"
- Materiał pomocniczy „Jak się wydostać z bańki filtrującej"

Zadania sprawdzające

Zadanie 1

Z poniższej listy wybierz czynności i rzeczy, na podstawie których możliwe jest profilowanie w sieci.

- ☐ przeglądane strony internetowe
- ☐ słowa wpisywane w wyszukiwarce internetowej
- ☐ informacje o sobie publikowane w sieci (np. wiek, płeć)
- ☐ „polubienia" w serwisie społecznościowym
- ☐ model procesora w komputerze
- ☐ informacje o geolokalizacji
- ☐ zawartość dysku twardego komputera
- ☐ zakupy przedmiotów w sklepach internetowych
- ☐ rodzaj przeglądarki internetowej

Słowniczek

Bańka filtrująca (ang. *filter bubble*) – sytuacja, w której na skutek działania określonego algorytmu osoba korzystająca z sieci otrzymuje wyselekcjonowane informacje, dobrane na podstawie informacji dostępnych na jej temat, takich jak lokalizacja czy historia wyszukiwania.

Ciasteczka (ang. *cookies*) – małe pliki tekstowe zapisywane na dysku użytkownika podczas korzystania ze stron WWW, które zapamiętują określone informacje o ustawieniach przeglądarki (np. wybrany język strony WWW, dane logowania) lub przesyłają pewne informacje z powrotem na serwery danej strony (np. ustawienia zabezpieczeń lub produkty w koszyku w sklepie internetowym). Ciasteczka mogą narażać użytkownika na wiele zagrożeń, gdyż działają w sposób niewidoczny i mogą zapamiętywać wiele wrażliwych informacji. Nowelizacja prawa telekomunikacyjnego nałożyła na właścicieli stron WWW obowiązek zamieszczenia w widocznym miejscu informacji o tym, że witryna korzysta z ciasteczek, oraz wskazówek na temat tego, jak można wyłączyć ich obsługę.

Geolokalizacja – określenie fizycznego położenia geograficznego osoby i urządzenia telekomunikacyjnego za pomocą systemu GPS lub adresu IP.

Profilowanie – oparty na określonych algorytmach mechanizm, który służy kategoryzowaniu ludzi według ich cech, zachowań, preferencji. Jest stosowany m.in. w marketingu internetowym w celu prezentowania reklam dopasowanych jak najściślej do potrzeb określonych użytkowniczek i użytkowników sieci, w branży bankowej i ubezpieczeniowej w celu oceny klienta, a także przez państwo w celu zwiększenia bezpieczeństwa (np. No Fly List w USA).

Czytelnia

1. Eli Pariser, *Uważaj na internetowe »bańki z filtrami«*, TED [dostęp: 24.05.2013]: http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles.html.
2. Małgorzata Szumańska, *Co warto wiedzieć o śledzeniu i profilowaniu w sieci*, Fundacja Panoptykon [dostęp: 22.12.2014]: http://cyfrowa-wyprawka.org/teksty/co-warto-wiedziec-o-sledzeniu-profilowaniu-w-sieci.
3. Kamil Śliwowski, Anna Obem, *Odzyskaj kontrolę w sieci. Odcinek I: przeglądarka*, Fundacja Panoptykon [dostęp: 19.10.2015] http://cyfrowa-wyprawka.org/teksty/odzyskaj-kontrole-w-sieci-odcinek-przegladarka.
4. Kamil Śliwowski, Anna Obem, *Odzyskaj kontrolę w sieci. Odcinek IV: Google*, Fundacja Panoptykon [dostęp: 19.10.2015] http://cyfrowa-wyprawka.org/teksty/odzyskaj-kontrole-w-sieci-odcinek-iv-google.
5. Kamil Śliwowski, Anna Obem, *Odzyskaj kontrolę w sieci. Odcinek V: alternatywne wyszukiwarki*, Fundacja Panoptykon [dostęp: 19.10.2015]: http://cyfrowa-wyprawka.org/teksty/odzyskaj-kontrole-w-sieci-odcinek-v-alternatywne-wyszukiwarki.
6. Jędrzej Niklas, Katarzyna Szymielewicz, *Jedwabny szlak danych*, Fundacja Panoptykon [dostęp: 23.06.2013]: http://www.panoptykon.org/wiadomosc/jedwabny-szlak-danych.

Ten materiał jest częścią projektu „Cyfrowa wyprawka" Fundacji Panoptykon.

Projekt współfinansowany ze środków Ministra Kultury i Dziedzictwa Narodowego.