

VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
INFORMATIKOS INSTITUTAS
PROGRAMŲ SISTEMŲ BAKALAURO STUDIJŲ PROGRAMA

Balso asistentų privatumo problemų analizė

Analysis of the privacy issues of voice assistants

Bakalauro baigiamasis darbas

Atliko:	Nerius Žarnauskas	(parašas)
Darbo vadovas:	lekt. Jonas Ragaišis	(parašas)
Darbo recenzentas:	dr. Darius Sauliūnas	(parašas)

Vilnius – 2022

Santrauka

Balso asistentai yra greitai tobulėjanti bei sparčiai pritaikoma technologija. Atsirandant vis daugiau interneto įrenginių, balso asistentai suteikia vartotojams naujas galimybes valdyti aplikacijas bei išmaniuosius namų prietaisus. Tačiau personalizuota vartotojų patirtis naudojantis šia technologija sukelia privatumo problemų. Pačių populiariausių balso asistentų kūrėjai renka milžiniškus kiekius asmeninės vartotojų informacijos ir dėl to yra atveriamos galimybės kenkėjiškiems asmenims išnaudoti šią technologiją vartotojams nepalankiais tikslais. Dėl to šiame darbe bus analizuojamos populiariausių balso asistentų - Google Assistant, Apple Siri ir Amazon Alexa, privatumo problemos, bei atliktas šių asistentų palyginimas pagal privatumą.

Raktiniai žodžiai: balso asistentai, privatumas, BDAR, pasitikėjimas balso asistentais, Siri, Google Assistant, Alexa

Summary

Voice assistant is a rapidly improving and widely adapting technology. The increase in number of Internet of Things devices with voice assistants provide new opportunities for users to operate their applications and smart home devices. However, the personalised user experience comes at a cost of user data privacy. The most popular voice assistants manufacturers collect large amounts of user personal data and therefore an opportunity for malicious activity is open. This work is focused on analysing the privacy problems of most popular voice assistants (Google Assistant, Siri and Alexa) and comparing them by privacy criteria.

Keywords: Voice assistants, privacy, GDPR, trust of voice assistants, Siri, Google Assistant, Alexa

TURINYS

IVADAS	4
1. KAS YRA BALSO ASISTENTAI?	6
1.1. Google assistant	7
1.2. Siri	7
1.3. Alexa	7
1.4. Tipinis balso asistento panaudojimo scenarijus	7
1.5. Balso asistentų atliekamos funkcijos pagal naudojamus įrenginius	8
2. PANAŠUMAI IR SKIRTUMAI	10
3. BALSO ASISTENTŲ PRIVATUMO PROBLEMOS	12
3.1. Susirūpinimas dėl privatumo užtikrinimo	12
3.2. Privatūs duomenys	12
3.3. Pasitikėjimas organizacijomis	13
3.4. BDAR	15
3.5. Vartotojų nuomonė apie balso asistentų privatumą	16
4. TYRIMAS	17
4.1. Privatumo užtikrinimo kriterijai	17
4.2. Google assistant privatumo įvertinimas	20
4.3. Apple Siri privatumo įvertinimas	22
4.4. Amazon Alexa privatumo įvertinimas	23
4.5. Balso asistentų palyginimas	24
4.5.1. Duomenų rinkimas	24
4.5.2. Duomenų bendrinimas	25
4.5.3. Duomenų apsauga	26
4.5.4. Duomenų teisės	26
4.5.5. Vartotojo kontrolė	27
4.5.6. Duomenų pardavinėjimas	28
4.5.7. Produkto apsauga	29
4.5.8. Reklamos ir duomenų stebėjimas	30
REZULTATAI	31
IŠVADOS	32
SANTRUMPOS IR SĄVOKŲ APIBRĖŽIMAI	38

Įvadas

Žmogaus ir kompiuterio sąveika įprastai būdavo įgyvendinama naudojant tokius išorinius įrenginius, kaip, klaviatūra, kompiuterio pelė ar liečiami ekranai. Šie prietaisai būdavo naudojami dėl to nes kompiuteriai nesugebėdavo suvokti šnekamosios kalbos ir suprasti žmogaus ketinimų. Tačiau per keletą pastarųjų metų tai ženkliai pasikeitė, dėl sparčiai tobulėjančių balso technologijų kompiuterinėse aplikacijose. Kadangi balsas yra vienas efektyviausių būdų raiškiai komunikuoti, balso technologijos stipriai keičia žmogaus ir kompiuterio sąveiką. Šiuo metu pati garsiausia inovacija naudojanti balso technologijas yra išmanieji balso asistentai (angl. Smart Personal Assistants). Balso asistentai yra technologija sugebanti surinkti vartotojo užklausas, jas suvokti ir atitinkamai atlikti užduotis. Kadangi balso asistentų valdymui nereikia naudoti rankų bei matyti ekrano, ši technologija padeda vartotojams įgyvendinti įvairias komandas užsiimant visiškai kita veikla. Taip pat balso asistentai padidina žmogaus ir kompiuterio bendravimo greitį nes įprastai žmogus kalba daug greičiau negu rašo [RWL+18]. Balso panaudojimas sąveikaujant su kompiuteriu atrodo daug natūresnis lyginant su išorinių prietaisų naudojimu ir dėl to yra kuriamas stipresnis socialinis ryšis su šia technologija [PFL19].

Šiuo metu balso asistentai yra integruojami į vis daugiau skirtingų prietaisų ir tampa įprasta namų valdymo technologija. Apie 4.2 milijardo balso asistentų buvo naudojami 2020 metais visame pasaulyje ir pranašaujama jog iki 2024 metų bus naudojami 8.4 milijardai balso asistentų - daugiau negu viso pasaulio gyventojų skaičius [LAR22]. Balso asistento populiarumą nulėmė funkcijų įvairovė, kurią suteikia šie prietaisai. Senesnės balsu valdomos technologijos suteikdavo tik mažą kiekį į patį įrenginį instaliuotų komandų. Tačiau dabartiniai balso asistentai naudoja interneto paslaugas bei pažengusias natūralios kalbos apdorojimo technologijas (angl. Natural Language Processing), kurios žymiai padidina balso asistentų galimybes. Dabartiniai balso asistentai yra daug patrauklesni dėl jų gebėjimo užmegzti žaismingus pokalbius. Taip pat, jie dažniausiai turi priskirtus vardus, kas vartotojams primena natūralų ir žmogišką bendravimą [PFL19]. Balso asistentai yra naudojami apsipirkinėti, sudėti dienos tvarkę, klausyti muzikos, radio, žinių, žaisti žaidimus, nustatyti žadintuvus, priminimus, atlikti skambučius, rašyti žinutes bei įgyvendinti daugelį kitų funkcijų. Dėl tokio greito balso asistentų augimo, artėjame prie naujo etapo, kai balso asistentai ne tik padės valdyti daugelį namie esančių įrenginių, tačiau visiškai juos pakeis. Pavyzdžiui, dabar balso asistentai yra naudojami kaip komunikavimo priemonė, atlikti skambučius bei rašyti žinutes, ir dėl to prietaisai su integruotais asistentais gali būti gera alternatyva laidiniams namų telefonams.

Populiarėjant balso asistentams, pačios vartotojų geidžiamiausios funkcijos sukelia įvairių saugumo problemų. Jos kyla dėl daugelio priežasčių: pačios svarbiausios balso asistentų funkcijos - valdymo balsu, sudėtingos architektūros, dirbtinio intelekto naudojimo bei priklausymo nuo daugelio kitų technologijų. Norint šių saugumo problemų išvengti reikia suprasti kokias rizikas sukelia balso asistento naudojamos technologijos. Nors daugelis šių technologijų turi tam tikrus saugumo ir privatumo užtikrinimo mechanizmus, vis dar egzistuoja didelis kiekis saugumo problemų, kurioms reiktų skirti dėmesio. Yra labai svarbu tvarkyti šias saugumo problemas, nes balso asistentai paliečia labai didelį gyvenimo sričių spektrą bei yra naudojami tokiose intymiose aplinkose kaip

naudotojų namai. Jau nekartą buvo pranešta apie vartotojų saugumo ir privatumo pažeidimus susijusius su balso asistento naudojimu. Vienas iš pavyzdžių buvo kai Amazon Alexa balso asistentas įrašė intymų pokalbį ir išsiuntė jį internetu [WOL18]. Tokie įvykiai gali sukelti vartotojų susirūpinimų saugumo bei privatumo užtikrinimo klausimais [CCJ18].

Dabartinėse balso asistentų integracijose privatumo problemos dar nėra išspręstos. Dėl to šiame darbe bus nagrinėjama kokios dabar egzistuoja privatumo problemos. Kadangi didžioji dalis naudojamų balso asistentų yra tokių didžiųjų technologijų gigantų kaip Google, Apple ir Amazon [SRD2022], dėl to šiame darbe bus siekiama apžvelgti būtent šių kompanijų kūriamų balso asistentų naudojimą, suprasti jų panašumus ir skirtumus, išsiaiškinti koku principu veikia šios technologijos ir svarbiausia atskleisti jų sukeltas privatumo problemas, bei suprasti kokia yra jų svarba. Taip pat remiantis literatūra apie balso asistentų vartotojų privatumo problemų susirūpinimą, bus sudaromas privatumo užtikrinimo kriterijų rinkinys, kuris padės palyginti, kuris balso asistentas yra saugesnis naudoti ir labiau užtikrina vartotojų privatumą.

Darbo tikslas

Šiuo darbu siekiama atskleisti privatumo problemas kylančias naudojantis vienais populiariausių balso asistentų Google assistant, Siri, Alexa. Taip pat atlikti šių balso asistentų palyginimą ir įvertinti kuri technologija yra saugiausia naudoti ir labiausiai užtikrina vartotojų privatumą.

Uždaviniai

1. Apžvelgti populiariausių balso asistentų veikimo principus, įvertinti jų panašumus ir skirtumus.
2. Išanalizuoti literatūrą susijusią su balso asistentų privatumo problemomis.
3. Sukurti balso asistentų privatumo vertinimo kriterijų rinkinį remiantis išanalizuotais skirtingų tipų privatumo pažeidimais.
4. Palyginti Google assistant, Siri ir Alexa balso asistentus pagal sukurtus vertinimo kriterijus.
5. Apibendrinti tyrimo rezultatus, pateikti išvadas ir rekomendacijas.

1. Kas yra balso asistentai?

Tai virtualios sistemos naudojančios balso atpažinimą, kalbą apdorojančius algoritmus bei balso sintezę (angl. voice synthesis) klausytis balso komandų ir suteikti aktualią informaciją arba atlikti funkciją automatizuojančią vartotojui įprastai daromus veiksmus rankiniu būdu. Visi šiame darbe nagrinėjami balso asistentai yra programinė įranga įrašyta į išmaniuosius telefonus arba būtent balso asistento funkcijas atlikti sukurtus įrenginius. Ši programinė įranga nuolat klausosi raktažodžio skirto aktyvuoti jos funkcionalumą. Išgirdus teisingą raktažodį, programa pradeda įrašinėti vartotojo balsą ir įrašą nusiunčia į serverį, kuris apdoroja garsą ir supranta tai kaip komandą atlikti tam tikrą veiksmą. Priklausomai nuo komandos, serveris suteikia balso asistentui reikiamos informacijos, pagal kurią balso asistentas žino ar reikia ištarti atsakymą vartotojui, ar įjungti tam tikrą programą, ar atlikti įvairiausių veiksmus naudojantis įrenginio galimybėmis. O galimybės, kurias gali panaudoti balso asistentai nuolat auga bei atsiranda vis daugiau įrenginių, automatizuojančių naujas vartotojų funkcijas.

Iš nagrinėjamų balso pagalbininkų Apple Siri asistentas yra atsiradęs seniausias, ši technologija buvo pradėta naudoti iOS įrenginiuose jau nuo 2010 [OBO21]. Vėliau sekė pradinė versija Google assistant, kuri dar tada vadinosi Google Now, išleista 2012 metais. Toks Google assistant, kurį žinome dabar, pasirodė Android įrenginiuose tik 2016 metais kartu su Google Nest įrenginiu skirtu balsu valdyti namuose įrengtus prietaisus [TIL22]. Ir Amazon Alexa balso asistentas buvo pradėtas naudoti 2014 metais [RUT22]. Kiekvienas asistentas turi savo unikalių funkcijų tačiau pagrindinė jų esmė yra tokia pati. Visi šie balso asistentai skiriasi nuo ankščiau egzistavusių balsu valdomų technologijų tuom, kad jie gali suprasti labai didelį kiekį komandų ir klausimų. Taip yra dėl to nes yra naudojamas Interneto ryšys. Kiekviena komanda yra nusiunčiama į centrinį duomenų analizavimo bloką, kuris turi daug skaičiavimo galios (angl. computing power) ir sugeba sugeneruoti tiksliausią atsaką į paduotą komandą. Ankščiau balsu valdomi prietaisai veikdavo remiantis tik lokaliai įrašytais komandomis ir atsakymais. Tačiau šių dienų kompiuterinės lingvistikos (angl. computational linguistics) technologijos, apdorojančios natūralią žmogaus kalbą, suteikė galimybę kurti balso asistentus, kurie generuoja greitus ir reikšmingus atsakymus.

Kadangi asmeniniai kompiuteriai ir mobilūs įrenginiai pasidarė daug pigesni ir galingesni, žmonių sąveika su įrenginiais sukūrė begales duomenų, kuriuos mokslininkai panaudojo apmokyti balso asistentus klausytis ir reaguoti į vartotojų užklausas žmogui suprantamu ir natūraliu būdu [CLO22]. Balso asistentai gali suprasti komandas suformuluotas įvairiausiais būdais ir teisingai interpretuoti ką vartotojas būtent norėjo pasakyti. Pavyzdžiui, paprašyti Google assistant atsiminti vietą, kur vartotojas priparkavo savo automobilį galima keliais būdais: "Atsimink kur aš pastačiau savo automobilį", "Aš prisiparkavau čia", "Palikau automobilį Vilniaus gatvėje", arba "Automobilis yra šiaurinėje aikštelės dalyje". Visos šios komandos variacijos suteiks tą patį rezultatą - Google atsimins, kur vartotojas pastatė automobilį ir sugebės atsakyti, apie tai paklausus. Pavyzdžiui, paklausus: "Kur aš palikau automobilį?" arba "Ar atsimeni, kur aš prisiparkavau?", bus gautas toks pat atsakymas. Šis natūralios kalbos supratimas suteikia galimybę kalbėti su kompiuteriais taip kaip kalbama su žmogumi ir padeda išvengti vartotojams atsiminti tikslias komandų formuluotes [STE22].

1.1. Google assistant

Google assistant yra Google sukurtas balso pagalbininkas naudojamas Android 5.0+ mobiliuose įrenginiuose, turinčiuose bent 1GB (gigabyte) RAM (angl. Random Access Memory) atminties arba Android 6.0+ su bent 1.5GB RAM atminties. Palaikomi mobilūs įrenginiai taip pat turi turėti mažiausiai 720 pikselių ekraną. Ši technologija yra integruota daugelyje kitų įrenginių, taip pat ir į Google gaminamus išmaniuosius garsiakalbius ir ekranus. Šis balso asistentas yra aktyvuojamas ištarus "Ok Google" arba "Hey Google" [TIL22].

1.2. Siri

Pirmasis balso asistentas atsiradęs daugelio vartotojų įrenginiuose buvo Siri. Šis balso asistentas buvo sukurtas Stanford Research institute ir buvo nupirktas Apple įmonės. Pirmiausia šis asistentas buvo prieinamas visiems iOS naudotojams kaip atskira mobili aplikacija, tačiau Apple išleidus iPhone 4S telefonų versiją Siri buvo integruotas į patį įrenginį. Dabar Siri yra integruotas į iPhone, iPad, iPod Touch, Apple Watch, HomePod, Apple TV ir Mac įrenginius. Šis balso asistentas yra įjungiamas panašiai kaip ir kiti asistentai, ištariant "Hey Siri" [OBO21].

1.3. Alexa

Alexa tai Amazon sukurtas balso asistentas integruotas į įvairius Amazon įrenginius. Pats populiariausias įrenginys, kurio valdymas paremtas Alexa balso asistentu yra Amazon Echo išmaniosios kolonėlės. Taip pat šį asistentą galime pasiekti naudojant Amazon Echo Show išmaniuosius ekranus, Amazon Fire plančetes, Amazon Fire TV bei Amazon Echo ausinukus [RUT22].

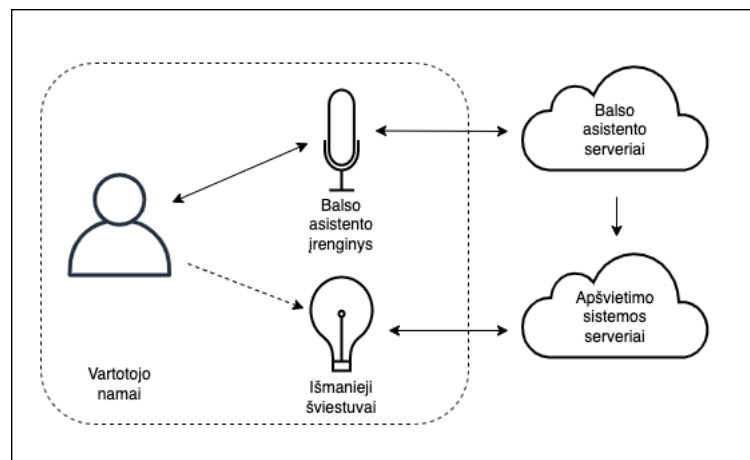
1.4. Tipinis balso asistento panaudojimo scenarijus

Balso asistentų funkcionalumas dažniausiai yra padalintas į kelias dalis, kurios vykdomos skirtingose vietose. Pavyzdžiui, balso apdorojimas ir komandų suvokimas yra dažniausiai vykdomas ne pačiame įrenginyje, o serveryje. Komandų įvykdymas įprastai vyksta įvairiausių interneto daiktų (angl. Internet of Things) įrenginių.

Balso asistentai nuolat įrašinėja garsą, kad galėtų tiksliai sureguoti į asistento pažadinimo raktažodį. Pavyzdžiui, Google asistento atveju - "Hey Google". Kai raktažodis yra ištariamas, balso asistentas įrašo vartotojo ištartą komandą ir siunčia duomenis į debesų sistemas (angl. Cloud-based systems), kur vyksta balso atpažinimo procesai. Balsas yra paverčiamas į virtualią formą, kuri yra lyginama su įvairių žodžių ir frazių virtualia forma, kad būtų galima atpažinti žmogaus ketinimą. Kad tai įgyvendinti, kompiuteris turi turėti duombazę skiemenų ir žodžių, įvairiomis kalbomis, kad būtų galima kuo tiksliau prilyginti žmogaus kalbą su virtualiais žodžiais. Toks įvesties duomenų tikrinimas su duombazėje esančiais žodžiais yra žinomas kaip modelio atpažinimas (angl. Pattern recognition) ir tai yra pagrindinis balso atpažinimo veikimo principas [SCA18]. Atpažinus vartotojo užklausą sugeneruojamas atsakymas ir išsiunčiamas į balso asistento įrenginį. Šie balso įrašai dažnai yra saugomi serveriuose ir gali būti naudojami balso atpažinimo algoritmų tobulinimui, nes

balso asistentų sistemos yra paremtos mašininio mokymo technologijomis. Mašininis mokymas (angl. Machine learning) tai dalis dirbtinio intelekto technologijos, kuri automatiškai kuria programas be žmogaus pagalbos. Programuotojai vietoje pilnos programos parašymo, sukuria sistemą, kuri atpažįsta modelius ir iš jų mokosi, ir tokiai sistemai duoda didelius kiekius duomenų, kurie yra naudojami programai tobulėti. Taigi dirbtinio intelekto programos neturi konkrečių taisyklių kaip jos turėtų veikti, tačiau jos ieško modelių tarp įvestų duomenų ir naudoja informacijos atpažinimui, kad patobulinti jau esantį programos funkcionalumą. Vienas iš būdų kaip mašininis mokymas gali padėti dirbtiniam intelektui, kuris naudojamas balso asistentuose yra didelis kiekis įvairiais akcentais ir tarmėmis tariamų balso įrašų [IBM20].

Taip pat, balso atpažinimas gali vykti pačiame balso asistento įrenginyje, nenaudojant jokių serverių ir nesaugant garso duomenų. Ne visi balso asistentai suteikia garsinį atsaką į vartotojo užklausas.



1 pav. Balso asistento panaudojimo scenarijus

Tipinis balso asistento panaudojimas su išmaniaisiais namų įrenginiais (angl. smart home) pavaizduotas 1 paveikslėlyje. Vartotojas ištaria komandą, pavyzdžiui, "Alexa, įjunk šviesas". Balso asistentas atpažįsta raktažodį "Alexa" ir garso įrašas "Įjunk šviesas" yra perduodamas serveriams. Tada balso atpažinimo technologijų pagalba garso signalas yra paverčiamas tekstu ir tekstas yra susiejamas su tam tikru veiksmu, šiuo atveju - šviesų įjungimu. Ir galiausiai serveris krepiasi į apšvietimo sistemos, instaliuotos vartotojo namuose, serverius, kurie įjungia šviesas. Pagal balso asistento įrenginio lokaciją, apšvietimo sistemos serveriai gali tiksliai nuspręsti, kurį šviestuvą įjungti. Taip pat serveris gali sugeneruoti žinutę, pavyzdžiui, "šviesos buvo įjungtos", ir nusiųsti jas atgal į balso asistento įrenginį. Tačiau šiuo atveju akivaizdžiai matosi sėkmingas komandos įvykdymas ir be balso asistento pranešimo.

1.5. Balso asistentų atliekamos funkcijos pagal naudojamus įrenginius

Mobilusis telefonas arba planšetė

- Komunikavimas. Skambinimas telefonu, SMS žinučių siuntimas, skambinimas su vaizdu, elektroninių laiškų siuntimas, kitų susirašinėjimo programėlių naudojimas žinutėms išsiųsti.

- Įrenginio kontrolė. WiFi ryšio įjungimas, Bluetooth ryšio įjungimas, "Do Not Disturb" režimo įjungimas, garsumo didinimas, ekrano ryškumo mažinimas, žibintuvėlio įjungimas, fotografavimas, informacijos ieškojimas naršyklėje, nuotraukų paieška, programėlių įjungimas
- Žadintuvo nustatymas, rezervacijų užsakymas, priminimų įrašymas, informacijos apie kamščius pranešimas.
- Prekių sąrašo sudarymas, pinigų aukojimas.
- Maršruto sudarymas, informacijos apie kamščius kelyje suteikimas, navigavimas kelionės metu.

Naudojantis išmaniaisiais garsiakalbiais arba ekranais

- Šviesų prigesinimas, kambario temperatūros nustatymas, muzikos garso padidinimas
- Žadintuvo nustatymas, rezervacijų užsakymas
- Skambinimas naudojantis komunikavimo programėlėmis.
- Durų atrakinimas, televizoriaus įjungimas, dulkių siurblio, kavos aparato, žoliapjovių, šaldytuvų valdymas.

Naudojantis išmaniaisiais televizoriais

- Programėlių įjungimas, informacijos paieška, filmų ir serialų įjungimas.
- Garso kontrolė, televizoriaus įjungimas, vaizdo sustabdymas, pratęsimas.

Naudojantis išmaniaisiais laikrodžiais

- Komunikavimas, elektroninių laiškų siuntimas, SMS bei kitų tipų žinučių siuntimas.
- Informacijos suteikimas apie širdies ritmą, nueitų žingsnių kiekį. Sporto treniruočių pradėjimas.

Naudojantis ausinėmis

- Baterijos pakrovimo lygio patikrinimas.
- Pašalinių garsų slopinimo įjungimas.
- Pašalinių garsų garsinimo režimo įjungimas.
- Ausinių prisilietimų kontrolės įjungimas.

[TIL22] [OBO21] [RUT22]

2. Panašumai ir skirtumai

Visi šie balso asistentai turi savų privalumų ir trūkumų tam tikrose srityse. 2021 metais buvo atliktas šiame darbe nagrinėjamų balso asistentų palyginimas pagal skirtingus šios technologijos aspektus: atsakymų tikslumą, palaikomų skirtingų interneto įrenginių kiekį, atpažįstamų komandų kiekį, pritaikymo galimybes, palaikomų kalbų kiekį [REW21].

Amazon Alexa:

- Alexa balso asistentas buvo įvertintas geriausiai pagal įrengnių pritaikymo kriterijų. Šis asistentas yra integruotas plačiausiame spektre įrenginių (daugiau nei 7400). Google Assistant palaiko apie 1000 įrenginių, Siri tik 50.
- Dėl Alexa ryšio su kitomis Amazon teikiamomis paslaugomis, šio balso asistento išskirtinumas yra prekinimosi internetu galimybės. Vartotojai turintys Amazon Prime prenumeratą gali lengvai užsakyti prekes, sekti bei atšaukti užsakymus naudojantis Alexa asistentu.
- Palyginus Alexa su kitais balso asistentais, buvo pastebėta, kad šio asistento atsakymų tikslumas yra prasčiausias. Tačiau yra pabrėžiama, kad šis asistentas palaiko labai didelį kiekį skirtingų komandų, dėl to pasiekti geresnį atsakymų tikslumą reikia daugiau laiko.
- Taip pat šio asistento minusas yra jog Alexa nėra instaliuotas mobiliuose įrenginiuose, priešingai nei Google Assistant ir Siri. Amazon suteikia galimybę parsisiųsti Amazon Alexa programėlę, tačiau naudojimosi patirtis yra žymiai prastesnė palyginus su konkurentų asistentais.

Siri:

- Siri yra labiausiai naudojamas balso asistentas iš šių trijų.
- Vienas iš Siri privalumų yra šio asistento suderinamumas su Apple produktais. Ištikimiams Apple vartotojams, kurie visada naudojo Apple produktus, Siri yra geriausias pasirinkimas dėl patogesnio naudojimo. Pavyzdžiui, naudojant Siri su išmaniaisiais namų įrenginiais, nereikia ištarti balso asistento raktažodžio, norint duoti asistentui užklausą. To negalima padaryti su Google Assistant ir Alexa.
- Taip pat Siri balso asistentas palaiko 21 skirtingą kalbą, kai Google Assistant tik 4, o Alexa 3. Tačiau palyginime yra pabrėžta, kad toks didelis kiekis kalbų yra palaikomas tik naudojant Siri per iPhone įrenginius.
- Vienas didžiausių Siri trūkumų yra tai jog šis asistentas palaiko labai ribotą kiekį mobilių aplikacijų, kurias galima valdyti balsu. Dėl to kad Apple skiria daugiausiai dėmesio būtent Apple įrenginių ir aplikacijų palaikymui, Siri nesuteikia vartotojams galimybės naudoti tokių mobilių aplikacijų, kaip Spotify ar Pandora.

Google assistant:

- Pagrindinis šio asistento išskirtinumas yra labai tikslūs atsakymai į vartotojų užklausas. Šis asistentas, skirtingai nei kiti, sugeba suprasti dvi komandas vienu metu, pavyzdžiui, asistentas gali prigesinti šviesas ir įjungti televizorių vartotojui pateikus tik vieną komandą.
- Taip pat dėl šio asistento suderinamumo su Google produktais, internetinė paieška yra vykdoma naudojant pačią populiariausią paieškos sistemą - Google. Tokiu būdu dar labiau pagerinant atsakymų tikslumą.

Tačiau nors ir kai kurie balso asistentai sugeba parinkti geresnius rezultatus ir atrodo patrauklesni vartoti, tai nebūtinai reiškia, kad jie suteikia geresnį saugumą ar užtikrina vartotojo privatumą. O saugumas ir privatumo užtikrinimas ne tik labiau paskatina vartotojus pradėti naudotis naujomis technologijomis, tačiau taip pat gerina pasitikėjimą visa organizacija [LVK+19].

3. Balso asistentų privatumo problemos

3.1. Susirūpinimas dėl privatumo užtikrinimo

Kadangi balso asistentai turi suteikti vartotojams kuo patogesnius būdus jais naudotis, ši technologija reikalauja visada klausytis aplinkos garsų. Šis faktas sukelia privatumo užtikrinimo klausimus. Turint žmogaus balso duomenis galima daug ką apie jį pasakyti, pavyzdžiui, žmogaus lytį, amžių, tautybę ar net sveikatos būklę [KFA+17]. Balso duomenys taip pat yra naudojami žmogaus identifikacijai [SHU15]. Taigi balsas yra laikomas jautriais žmogui duomenimis ir teisinių sistemų kaip Bendrasis duomenų apsaugos reglamentas (BDAR) arba GDPR (angl. general data protection regulation) pritaikymas yra svarbus balsu valdomom technologijom. Pavyzdžiui BDAR reikalauja, kad vartotojas duotų sutikimą rinkti jo duomenis, ir kad sistemos, renkančios duomenis apie vartotojus, atsižvelgtų į vartotojų privatumą pagal tam tikras taisykles. Pagal BDAR duomenų rinkėjai turi apsaugoti vartotojų teises ir laisves naudodami jų duomenis. Duomenų apsauga yra kiekvienos, duomenis renkančios, sistemos įsipareigojimas [EUR18]. Tačiau nors ir egzistuoja tokie reglamentai kaip BDAR, vartotojai nėra apsaugoti nuo jų duomenų vagysčių, nes asmenys, siekiantys išnaudoti balso asistentų saugumo trūkumus, panaudoja šią technologiją, kaip pasiklausymo įrangą [GRE17].

3.2. Privatūs duomenys

Balso savininko tapatybė yra įprastai laikoma pačia privačiausia vartotojo informacija, tačiau ir ne biometriniai duomenys gali būti jautrūs vartotojui ir dėl to šiuos duomenis reikia taip pat apsaugoti [EUC22]. Vartotojai nori kontroliuoti kaip jų biometriniai ir ne biometriniai duomenys yra saugomi, apdorojami arba bendrinami [LZS18].

Jeigu balso atpažinimas būtų naudojamas pačiuose balso asistentus turinčiuose įrenginiuose tai privatumą užtikrinti būtų daug paprasčiau. Tačiau dėl įrenginio galimybių limitų, balso atpažinimas pačiame įrenginyje yra taip pat ribotas. Taip pat balso asistentų gamintojai dažniausiai renkasi centralizuotą sprendimą, kad visi procesai būtų atliekami vienoje vietoje. Žinoma mobiliųjų įrenginių galingumas vis auga ir dėl to artimoje ateityje balso atpažinimo algoritmai potencialiai bus implementuoti pačiuose įrenginiuose [HSP+18]. Tai turėtų suteikti vartotojams daugiau kontrolės tvarkyti privačius balso duomenis. Tačiau net ir įgyvendinus balso atpažinimą mobiliuose įrenginiuose, nebus galima pilnai palaikyti balso asistento funkcionalumo nenaudojant duomenų apdorojimo serveryje.

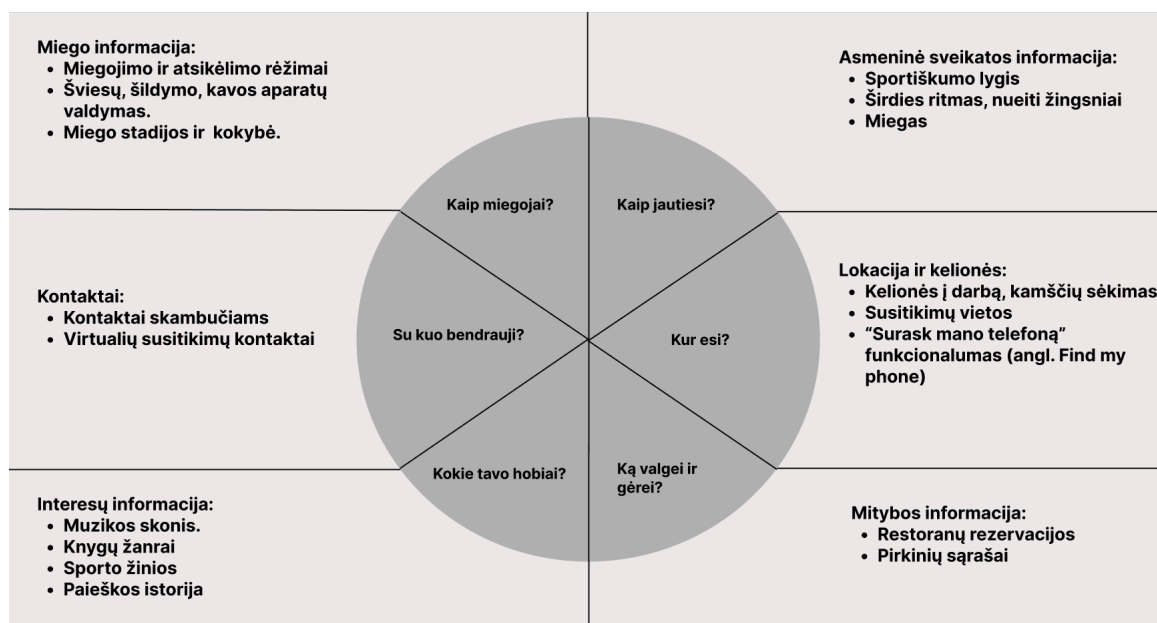
Žinoma buvo apsvaistytos galimybės techninės įrangos pagalba apsaugoti privačius duomenis. Buvo pasiūlyta architektūra naudojanti Intel SGX technologiją vadinama VoiceGuard [BFR+18]. SGX leidžia apibrėžti privačias atminties vietas, kurių turinys yra apsaugotas ir nepasiekiamas jokio kito proceso vykstančio už tos privačios atminties vietos ribų. VoiceGuard architektūroje, balso charakterizavimas yra atliekamas toje privačioje SGX atminties dalyje ir dėl to vartotojo balso duomenys nėra pasiekiami serverių, bei duomenys serveryje yra nepasiekiami vartotojui. Tačiau tokie sprendimai kaip VoiceGuard turi apribojimų: yra būtina SGX techninė

įranga, privačios atminties dalies dydžio apribojimai neleidžia atlikti sudėtingų balso atpažinimo operacijų.

3.3. Pasitikėjimas organizacijomis

2018 metais buvo apskaičiuota, jog 80 procentų visų egzistuojančių duomenų buvo sukurti per pastaruosius du metus [KUM18]. IoT įrenginiai dar labiau paspartino duomenų surinkimą, saugojimą ir analizavimą. Dirbtinio intelekto pritaikymas šiems duomenims padidino jų vertę ir sudarė galimybę kompanijom uždirbti pinigų juos panaudojant reklamoms ir rekomendacijoms [GCM16] [RST16].

Tačiau iš vartotojo perspektyvos labai trūksta aiškumo susijusio su tokiais dideliais kiekiais saugomų duomenų [LZS18]. Organizacijos dažnai tiesiogiai neapibrezia kokiais tikslais ir metodais yra saugomi vartotojų duomenys. Taip pat, yra neaišku kur ir kokiais tikslais duomenys yra panaudojami trečių šalių platformose. Nors tokiais būdais surinkinėjami duomenys gali atrodyti nepavojingi, tačiau šiais laikais vykstant privatumo įsilaužimams, yra įmanoma išgauti daug informacijos apie konkretų asmenį [KBL+16].



2 pav. Balso asistentų pasiekiamą informaciją

2 paveiksliuke matome kokių tipų informacija yra pasiekiamą balso asistentų per prijungtus įrenginius ir aplikacijas. Šiame paveiksliuke pateikta tik dalis informacijos tipų, kuriuos gali pasiekti balso asistentai, naudojantis atitinkamom jų funkcijom. Miego bei sveikatos informacija yra pasiekiamą tų naudotojų, kurie nešioja išmaniuosius laikrodžius, pavyzdžiui, Fitibit laikrodžiai palaiko Google Assistant balso asistentą bei Apple išmaniuosiuose laikrodžiuose galima naudotis Siri asistentu. Taip pat žinome, kad balso asistentai yra naudojami kaip komunikacijos priemonė, dėl to jie naudoja kontaktų informaciją. Naudojantis paieškos sistema, klausantis muzikos per tokias aplikacijas kaip Spotify, naršant knygas per balso asistentą suteikiama informacija apie vartotojo interesus. Sudarinėjant pirkinių sąrašus ar atliekant restorano rezervacija balsu suteikiama

informacija apie vartotojo mitybos įpročius. Taip pat suteikiama vartotojo lokacijos informacija naudojantis maršruto sudarymo aplikacijomis, pavyzdžiui, Google Maps, sudarant susitikimus kalendoriuje, ar praradus įrenginį naudojant telefono suradimo funkcionalumą, Siri atveju - "Surask mano telefoną" (angl. Find my phone) [TIL22] [OBO21] [RUT22].

Asmeninė identifikacijos informacija ir asmeninė sveikatos informacija yra du informacijos tipai surenkami balso asistentų įrenginių [DWK15]. Nors IoT įrengių gamintojai pripažįsta ir pabrėžia jog surinkinėja duomenis savo terminų ir sąlygų rinkinyje, tačiau tų įrenginių integracija su balso asistentais sukelia naujų pažeidžiamumų [SZK+17] [KBL+16] [RST16].

Jeigu įrenginio balso asistentas yra sukonfiguruotas, esant atitinkamam atstumui nuo įrenginio, galima išstarti komandas ir pasiekti tą informaciją. Identifikacijos informacija, tokia kaip socialiniai duomenys, vietovė, pirkimų istorija, hobiai bei kiti vartotojo interesai, gali būti išgauta iš prijungtų prietaisų kaip išmanūs laikrodžiai [GRA17]. Sveikatos informacija, gali sudaryti, nueitų žingsnių kiekis, širdies ritmas, miego duomenys. Prieiga prie tokių duomenų sukelia rimtą grėsmę duomenų, sugeneruotų balso asistentų, privatumui [WMS16].

Daugeliui vartotojų pasitikėjimas yra savybė kurią reikia užsitarnauti [LZS18]. Vartotojų pasitikėjimo stiprinimas yra svarbus norint integruoti balso asistentus į vis daugiau skirtingų įrenginių, kurie būtų naudojami privačioje naudotojų aplinkoje [ALH18]. Tačiau balso asistentai yra patraukli technologija vartotojams dėl suteikiamų naujų galimybių ir patogumo. Jie palengvina kasdienes darbus, namų ruošą bei sveikatos būklę. Nors daugelis vartotojų žino, kad šitie privatumai gali kainuoti jų privatumą, vartotojai vis tiek renkasi naudoti šią technologiją [LZS18]. Balso asistentų įrenginiai kaip Amazon Echo yra sujungti su daugeliu skirtingų Amazon produktų (Prime, Music Unlimited, Video, Audible), kurie jau turi vartotojų pasitikėjimą [AND17]. Tačiau duomenų kiekis, kuriuos vartotojai yra pasirūšę atskleisti yra ribotas ir ta riba priklauso nuo pasitikėjimo balso asistentais.

Pasitikėjimas apibrezia, kaip mes esame užtikrinti jog privatūs duomenys bus apsaugoti ir naudojami tik dėl bendrai sutartų tikslų. Pagal Technische Universiteto Vokietijoje mokslininkus [DWK15], pasitikėjimas yra skaidomas į keturias kategorijas:

1. Įrenginio pasitikėjimas (angl. Device Trust)
2. Duomenų apdorojimo pasitikėjimas (angl. Processing Trust)
3. Duomenų apsikeitimo pasitikėjimas (angl. Connection Trust)
4. Sistemos pasitikėjimas (angl. System Trust)

Balso asistentų atveju, kiekviena ši kategorija sukelia naujų sunkumų. Pasitikėjimas įrenginiu dažniausiai yra pasiekiamas griežtais testavimo procesais [RPP+18]. Tačiau dar visai neseniai matėme, kaip Amazon Echo balso išmanusis garsiakalbis su integruotu balso asistentu, atsitiktinai paskambino vienam iš vartotojų kontaktų ir įrašė pokalbį [JAO18]. Tokie įvykiai gali sumažinti vartotojų pasitikėjimą organizacija [CCJ18].

Duomenų apdorojimo pasitikėjimas yra panašus į sąveiką su internetu, kai nesitikima jog visi įrenginiai veiks tobulai visais atvejais. Kai rizika nėra didelė, vartotojai toleruoja tam tikrą lygį nesuderinamumo. Pavyzdžiui, jeigu balso asistentas įjungia kitokią dainos versiją, negu vartotojas prašė, tai nėra didelė problema vartotojui. Tačiau didelės rizikos atveju, kai balso asistentas

naudojamas atlikti mokėjimus, duomenų apdorojimo pasitikėjimas yra daug svarbesnis. Jeigu balso asistentas įgyvendina klaidingą prikimą ir tokiu būdu vartotojas nukenčia finasiškai, tada ženkliai krenta pasitikėjimas duomenų apdorojimu. Balso asistentų kūrėjai yra atsakingi sumažinti klaidingų pirkimų kiekį, jeigu pirkimas balsu taps vienu pagrindiniu prekinimosi internetu būdu [TOK+17].

Duomenų apsikeitimo pasitikėjimas yra taip pat svarbus, norint pasiekti kuo didesnį balso asistentų naudotojų kiekį. Nors vartotojai gali pasitikėti Amazon ar Google, tačiau bet kokia indikacija, jog vartotojų duomenys gali būti nutekinti trečių šalių platformoms, gali stipriai sumažinti pasitikėjimą pačiomis platformomis [LZS18]. Trečių šalių aplikacijų, kaip Alexa skills ar Google Actions, naudojimas sukelia dar daugiau naujų problemų norint sukurti duomenų apsikeitimo pasitikėjimą.

Pasitikėjimas sistema yra vienas sunkiausių iššukių įrenginių gamintojams. Organizacijos dažnai nėra suinteresuotos suteikti daug informacijos apie įrenginiuose vykstančius procesus, dėl saugumo priežasčių. Įsilaužėliai gali pasinaudoti pateikta informacija, kad lengviau įsilaužtų ir pažeistų duomenų privatumą. Taip pat dėl naudojamų gilaus mokymosi neuroninių tinklų apdorojant vartotojo balsą, dažnai yra tiesiog neįmanoma paaiškinti kol balso asistentas atsakė į klausimą būtent tam tikru būdu dėl to nes neuroniniai tinklai turi tūkstančius įvesčių ir tūkstančius modelių sluoksnių [WSK+18]. Ši problema galioja ne tik balso asistentams, bet ir visiems įrenginiams naudojančiams dirbtinį intelektą.

3.4. BDAR

Pastangos spręsti vartotojų pasitikėjimo problemas yra aktualu organizacijom, tačiau dar svarbiau yra apsaugoti vartotojų duomenis įstatymiškai. Vienas didžiausių pokyčių duomenų apsaugos įstatymuose buvo BDAR, kuris atsirado 2018 metų gegužę.

BDAR buvo vienas didžiausių pasikeitimų Europos duomenų apsaugos teisėje per daugiau nei 20 metų. Sparti naujų technologijų pažanga pareikalavo pergalvoti esamas taisykles, bei sukurti naują reglamentą, kuris atsižvelgtų į nuolat atsirandančias naujas technologijas, įskaitant ir IoT, dirbtinį intelektą bei Debesų inžineriją. Šis pokytis stipriai pakeitė organizacijų požiūrį į duomenų surinkimą ir vartotojų asmeninių duomenų naudojimą [HPA17]. Dėl to dabar visuose balso asistentų taisyklių ir sąlygų dokumentuose (angl. Terms and Conditions) turi būti aiškiai aprašyta kokie duomenys bus saugojami ir kokiais tikslais naudojami, bei vartotojai turi būti informuoti apie bet kokius taisyklių ir sąlygų pokyčius. BDAR taisyklių rinkinyje yra keletas punktų, kurie labiausiai taikomi balso asistentų technologijoms.

- Prieigos teisė (angl. Right of Access). Galimybė pasiekti visą organizacijos saugomą asmeninę informaciją.
- Atnaujinimo teisė (angl. Right of Rectification). Užtikrina, jog visi neteisingi ar pasenę duomenys bus atnaujinti.
- Ištrinimo teisė (angl. Right of Erasure). Užtikrina, jog bet kokie vartotojo asmeniniai duomenys gali būti ištrinti, vartotojui pareikalavus.
- Duomenų apdorojimo ribojimo teisė (angl. The right to restriction of processing). Užtikrina

vartotojo asmeniniai duomenys bus naudojami tik bendrai nutartais tikslais.

- Duomenų perkeliamumo teisė (angl. Right to Data Portability). Suteikia galimybę vartotojams pasiimti asmeninius duomenis paliekant organizaciją.
- Prieštaravimo teisė (angl. Right to Object). Galimybė pareikalauti nustoti naudoti vartotojo asmeninius duomenis.
- Duomenų privatumo projektavimas (angl. Data Privacy by Design). Reikalavimas, jog duomenų privatumo užtikrinimas turi būti planuojamas projektuojant produktą.
- Automatizuotas individualus sprendimų priimimas, iskaitant ir profiliavimą. (angl. Automated Individual Decision Making, including profiling). Užtikrina, jog vartotojų asmeniniai duomenys nebus grupuojami siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius aspektus, pavyzdžiui, pomėgius, interesus, darbo rezultatus, ekonominę situaciją. Tai yra vienas sunkiausiai įgyvendinimų reikalavimų, nes pagrindinis balso asistentų gamintojų pajamų šaltinis yra profiliuotų vartotojo duomenų pardavinėjimas marketingo kompanijoms.

3.5. Vartotojų nuomonė apie balso asistentų privatumą

Mičigano Universiteto mokslininkai atliko tyrimą apklausdami balso asistentų naudotojus ir nenaudotojus (angl. non-users). Naudotojai buvo apklausti apie jų patirtis naudojantis balso asistentais, jų požiūrį apie šios technologijos privatumo klausimus, bei jų susirūpinimą balso asistentų saugumu. Asmenys nenaudojantys balso asistentų buvo apklausti siekiant išsiaiškinti dėl kokių priežasčių jie vengia naudoti balso asistentus bei kaip stipriai jų sprendimą lemia privatumo klausimai [LZS18].

Šios apklausos rezultatai patvirtino, jog privatumo neužtikrinimas yra pagrindinis žmonių, vengiančių naudoti balso asistentus, veiksnys. Apklaustieji teigė, kad tas faktas, jog namie yra įrenginys, kuris gali rinkti įvairiausią informaciją, būti panaudojamas pasiklausymui, kenksmingiems tikslams, verčia jaustis nesaugiai. Taip pat apklaustieji pareiškė susirūpinimą dėl vartotojo ir organizacijos sutarties rinkti ir dalintis duomenimis, bei pranešimą apie sutarties pokyčius bei duomenų įsilaužimus. Jų nuomone, sutartis gali keistis jiems nepranešus, ko pasekoje vartotojai nebūtų informuoti apie naujų duomenų rinkimą. Tai pat apklaustieji, žinodami kiek daug informacijos renka interneto produktus kuriančios kompanijos, teigė jog nenori, askleisti dar daugiau asmeninės informacijos į interneto platybes. Apklausius vartotojų ir ne vartotojų nuomones apie balso asistentų renkamų duomenų naudojimo tikslinės auditorijos reklamoms (angl. targeting advertising), abi grupės buvo susirūpinusios šiuo klausimu ir teigė jog jaučiasi nesaugiai, nežinant kaip jų informacija, parduota reklamų kompanijoms, gali būti panaudota prieš pačius vartotojus, bei pareiškė susirūpinimą dėl nepakankamos tikslinės auditorijos reklamų kontrolės. Didžioji dalis apklaustųjų buvo stipriai susirūpinę trečių šalių įsitraukimo į balso asistento renkamų duomenų valdymą klausimais ir teigė, jog tikisi, kad duomenys bus renkami tik balso asistento organizacijos.

Nors ir keletas apklaustųjų buvo įsitikinę niekada nenaudoti balso asistentų dėl šių priežasčių, dalis jų teigė jog ateityje svarsto įsigyti šią technologiją jeigu šios problemos bus išspręstos.

4. Tyrimas

4.1. Privatumo užtikrinimo kriterijai

Norint palyginti skirtingų balso asistentų privatumą reikia kriterijų rinkinio, pagal kurį bus atlikta lyginamoji analizė. Tam, kad šis privatumo kriterijų rinkinys padėtų lengvai palyginti skirtingas balso asistentų integracijas, buvo atsižvelgta į pačius svarbiausius ir lengvai suprantamus privatumo aspektus. Kriterijų rinkinys buvo sudarytas atsižvelgiant į privatumo užtikrinimo naudą iš kelių perspektyvų: vartotojo perspektyvos (atsižvelgiant į ankščiau išvardytus vartotojų privatumo susirūpinimus balso asistentų technologijose) ir organizacijų perspektyvos (atsižvelgiant į privatumo įtaką organizacijų pasitikėjimui). Taip pat kuriant šiuos kriterijus buvo atsižvelgta į 8 BDAR reglamento punktus, ankščiau minėtus šiame dokumente.

Nagrinėjant vartotojų privatumo susirūpinimus, pasitikėjimą organizacijomis bei BDAR reglamentą buvo sudaryti 52 klausimai pagal kuriuos buvo daromas balso asistentų palyginimas. Šie klausimai buvo sugrupuoti į 8 kriterijus pagal skirtingą privatumo užtikrinimo aspektą.

1. **Duomenų rinkimas.** Vienas didžiausių vartotojams kylančių privatumo klausimų naudojantis balso asistentais yra - kokie yra renkami asmeniniai duomenys? Dėl to į šį kriterijų buvo įtraukti klausimai apie tai kokius asmeninius duomenis renka organizacija (Identifikacijos duomenys, biometrinė informacija, vartotojo sveikatos duomenys, geografinė padėtis bei kita jautri vartotojų informacija - religija, politinis požiūris, rasė ar seksualinė orientacija). Tai pat svarbu buvo įtraukti klausimą ar organizacija renka duomenis tik su vartotojo sutikimu, dėl to nes šio aspekto neaiškumas yra viena iš priežasčių kodėl žmonės nesirenka naudoti balso asistentų. Galiausiai dėl vartotojų susirūpinimų dėl trečių šalių įsitraukimo į vartotojų duomenų rinkimą bei naudojimą buvo įtrauktas klausimas vertinantis ar trečių šalių sistemos taip pat renka asmeninius vartotojo duomenis:

- Ar renkama identifikacijos informacija?
- Ar renkama biometrinė informacija ir sveikatos duomenys?
- Ar renkami geografinės padėties duomenys?
- Ar renkama jautri naudotojų informacija?
- Ar duomenys renkami tik su vartotojo sutikimu?
- Ar vartotojų asmeninė informacija yra renkama naudojant trečių šalių sistemas?

2. **Duomenų bendrinimas.** Duomenų bendrinimas su trečių šalių sistemomis yra taip pat vienas didžiausių vartotojų privatumo susirūpinimų, bei informacija apie duomenų bendrinimą daro įtaką duomenų apsaugos pasitikėjimui tarp vartotojų ir organizacijos. Remiantis BDAR - Duomenų apdorojimo ribojimo teisės punktu vertiname ar kompanija pateikia priežastis kodėl yra bendrinami vartotojo duomenys su trečių šalių organizacijomis bei ar yra ribojamas bendrinamų vartotojo duomenų naudojimas:

- Ar renkama informacija yra bendrinama su trečių šalių sistemomis?
- Ar nurodyti duomenų bendrinimo su trečių šalių sistemomis tikslai?
- Ar vartotojo duomenų, bendrinamų su trečių šalių sistemomis, naudojimas yra ribotas pagal pasirašytus kontraktus su kitomis organizacijomis?

3. **Duomenų apsauga.** Remiantis BDAR - Duomenų privatumo projektavimo punktu vertinama ar organizacija naudoja duomenų apsaugos mechanizmus. Vertinama dalis pačių populiariausių duomenų saugumo užtikrinimo praktikų: kelių veiksmų autentifikavimas, duomenų šifravimas, vartotojo tapatybės patvirtinimas, prieigos prie duomenų ribojimas. Taip pat kadangi organizacijos galimai bendrina informaciją su trečių šalių kompanijom, buvo įtrauktas punktas išsiaiškinti ar organizacija reikalauja saugumo principų laikytis ir kitom organizacijom naudojančiom vartotojų duomenis. Galiausiai remiantis vartotojų susirūpinimu apie organizacijos pranešimus vartotojam dėl duomenų apsaugos pažeidimų buvo įtrauktas vertinimas ar organizacija informuoja vartotojus apie duomenų įsilaužimus:
- Ar vartotojo tapatybė yra patvirtinama su papildoma identifikavimo informacija?
 - Ar yra kelių veiksmų (angl. multi-factor) paskyros apsauga?
 - Ar trečių šalių sistemos turinčios prieigą prie vartotojo duomenų turi palaikyti tokius pačius saugumo užtikrinimo principus kaip ir pati organizacija?
 - Ar darbuotojų prieiga prie duomenų yra ribota?
 - Ar fizinis duomenų prieinamumas yra ribotas?
 - Ar duomenų perdavimo metu informacija yra užšifruota?
 - Ar saugomi duomenys yra užšifruoti?
 - Ar organizacija informuoja vartotojus apie įvykusius duomenų įsilaužimus?
4. **Duomenų teisės.** Šiuo aspektu vertinimo kriterijai buvo sukurti remiantis daugeliu anksčiau minėtų BDAR punktų (Prieigos teisė, atnaujinimo teisė, ištrinimo teisė, duomenų perkeliavimo teisė).
- Ar vartotojai turi nuosavybės teisę į savo asmeninius duomenis?
 - Ar vartotojai turi galimybę pasiekti ir peržiūrėti apie juos saugomus duomenis?
 - Ar vartotojai turi galimybę keisti apie juos saugomus duomenis?
 - Ar vartotojai turi galimybę ištrinti apie juos saugomus duomenis?
 - Ar ištrynus naudotojo paskyra, kartu yra ištrinami ir jo duomenys?
 - Ar duomenys yra ištrinami kai jie nebėra naudojami?
 - Ar yra galimybė vartotojui parsisiųsti savo asmeninę informaciją?
5. **Vartotojo kontrolė.** Remiantis vartotojų susirūpinimais dėl neaiškumo ar egzistuoja galimybės kontroliuoti jų duomenų rinkimą bei naudojimą šiame vertinime būtent į tokio tipo klausimus ir yra atsižvelgiama. Remiantis BDAR punktu - Automatizuotas individualus sprendimų priimimas, iskaitant ir profiliavimą, vertinama ar vartotojų duomenys nėra kombinuojami ir jeigu yra, tai ar ta informacija yra laikoma kaip identifikavimo. Dėl vartotojų susirūpinimų pranešimu apie jų duomenis klausimais buvo vertinta ar administracinėms institucijoms pareikalavus duomenų apie vartotojus, pasikeitus duomenų surinkimo praktikoms ar pasikeitus duomenų rinkimo priežastims apie tai pranešama vartotojams ir ar prašoma sutikti su naujom sąlygom. Taip pat remiantis BDAR punktu - Prieigos teise, buvo vertinama ar vartotojai gali pasiekti jų asmeninę informaciją bendrinamą su kitomis organizacijomis.
- Ar vartotojai gali kontroliuoti apie juos renkama informaciją naudojant privatumo nustatymus?

- Ar naudotojai gali atsisakyti atskleisti savo duomenis kitoms organizacijoms?
- Ar informacija yra panaudojama tik tiems tikslams dėl kurių ji buvo rinkta?
- Ar organizacija gali sujungti duomenis su papildoma informacija iš trečių šalių šaltinių?
- Ar kombinuota informacija yra laikoma identifikacijos informacija?
- Ar vartotojams pranešama jeigu pasikeičia priežastis dėl kurios duomenys yra renkami?
- Ar organizacija prašo vartotojų iš naujo sutikti su sąlygomis ir taisyklėmis jeigu pasikeičia duomenų surinkimo praktikos?
- Ar vartotojai gali paprašyti gauti su kitom organizacijom bendrinamą asmeninę informaciją?
- Ar vartotojui pranešama jeigu jo duomenų pareikalauja vyriausybė arba kitos teisinės institucijos?

6. Duomenų pardavinėjimas. Remiantis vartotojų susirūpinimu dėl jų duomenų bendrinimo ar pardavinėjimo su kitomis organizacijomis vertiname ar organizacijos pardavinėja vartotojų duomenis. Taip pat atsižvelgiant į tai, kad duomenys gali būti perduoti ne tik tiesiogiai, bet ir įvykstant organizacijų susijungimams, įsigyjimams ar bankroto atvejais, vertiname ar tokie atvejai yra galimi nagrinėjamose organizacijose. Taip pat atsižvelgiant į vartotojų susirūpinimus dėl pranešimų apie pokyčius su jų duomenimis, vertiname ar organizacijos praneša apie duomenų perdavimą kitai organizacijai. Remiantis BDAR ištrinimo teisės punktu vertiname ar vartotojai turi galimybę ištrinti savo duomenis prieš atiduodant juos kitai organizacijai. Taip pat remiantis BDAR - duomenų privatumo projektavimo punktu vertiname ar duomenys yra perduodami anonimišku formatu, kokie naudojami anonimizavimo mechanizmai, bei ar organizacija identifikuoti perduotus duomenis.

- Ar vartotojų asmeniniai duomenys nėra pardavinėjami trečių šalių organizacijoms?
- Ar vartotojų duomenys gali būti perduoti trečių šalių organizacijoms vykstant orgranizacijų susijungimams, įsigyjant naują kompaniją arba bankroto atveju?
- Ar naudotojai yra informuoti įvykus duomenų perdavimui kitai orgranizacijai?
- Ar vartotojai gali ištrinti savo informaciją prieš perduodant ją kitai organizacijai?
- Ar vartotojų duomenys yra perduoti anonimišku formatu?
- Ar organizacija atskleidžia kokiais būdais anonimizuojami vartotojo duomenys?
- Ar organizacija draudžia trečių šalių organizacijoms identifikuoti duomenis?

7. Produkto apsauga. Remiantis BDAR - duomenų privatumo projektavimo punktu vertiname ar organizacija naudoja produktų apsaugos mechanizmus (vartotojų sąveikų moderavimas, komunikavimo draudimas su nepatikimais vartotojais, informacijos viešinimo vengimas). Šiuo aspektu yra vertinama sąveikos tarp vartotojų (Naudojant balso asistentų komunikavimo funkcijas) saugumas.

- Ar vartotojai gali sąveikauti su nepatikimais vartotojais?
- Ar profilio informacija turi būti bendrinama norint socializuotis su kitais vartotojais?
- Ar asmeninė informacija turi būti rodoma viešai?
- Ar vartotojai gali kontroliuoti kokia informacija yra atvaizduojama kitiems vartotojams?

- Ar vartotojų sukurtas turinys yra peržiūrimas ir įvertinimas?
- Ar vartotojų sukurtas turinys, turintis asmeninės informacijos, yra išfiltruojamas prieš jį pavišinant?
- Ar yra renkami duomenys apie sąveikas tarp vartotojų?

8. **Reklamos ir duomenų stebėjimas.** Nagrinėjant vartotojų privatumo susirūpinimus paaiškėjo, jog vartotojų asmeninių duomenų bendrinimas su trečių šalių marketingo organizacijoms, bei tų duomenų naudojimas personalizuotoms reklamoms lemia vartotojų apsisprendimą vengti naudoti balso asistentų technologijas. Dėl to šiuo aspektu vertiname ar organizacija dalinasi duomenimis su trečių šalių marketingo organizacijomis, ar duomenys naudojami personalizuotoms reklamoms, bei kokia suteikiama vartotojui kontrolė atsisakyti reklamų ar marketingo komunikacijos. Taip pat remiantis BDAR punktu - automatizuotas individualus sprendimų priimimas, iskaitant ir profiliavimą, buvo vertinama ar vartotojo duomenys yra profiluojami personalizuotoms reklamoms.

- Ar asmeninė informacija yra bendrinama trečių šalių marketingo organizacijoms?
- Ar kuriami duomenų profiliai skirti personalizuotoms reklamoms?
- Ar vartotojo informacija yra naudojama reklamoms kitose trečių šalių sistemose?
- Ar vartotojai gali atsisakyti personalizuotų reklamų?
- Ar vartotojai gali atsisakyti marketingo komunikacijos?

1 lentelė. Privatumo kriterijų rinkinys

Duomenų rinkimas	Kokie duomenys yra renkami?
Duomenų bendrinimas	Kokie duomenys yra bendrinami?
Duomenų apsauga	Kaip duomenys yra apsaugomi?
Duomenų teisės	Kokias teises turi vartotojai į renkamus duomenis?
Vartotojo kontrolė	Ar galima vartotojui kontroliuoti kaip yra naudojami jo duomenys?
Duomenų pardavinėjimas	Ar duomenys yra pardavinėjami?
Produkto apsauga	Kaip yra apsaugomi produktai?
Reklamos ir duomenų stebėjimas	Ar duomenys naudojami reklamoms ir stebėjimui?

4.2. Google assistant privatumo įvertinimas

Šiame vertinime yra atsižvelgiama tik į viešai prieinamą informaciją apie Google produktus. [GOO22a] [GOO22b] [GOO22c] [GOO22d] [GOO22e] [GOO22f] [GOO22g] [GOO22h]

Google sąlygose yra teigiama, jog šios organizacijos kuriamos paslaugos padeda milijonams žmonių kasdien ieškoti naujos informacijos ir sąveikauti su pasauliu vis naujais būdais. Dėl to, Google pabrėžia, kad ši organizacija supranta kokia yra visiems vartotojams tinkančio privatumo užtikrinimo svarba. Sąlygose rašoma, kad Google vadovaujasi privatumo užtikrinimo principais kuriant naujus produktus, atsirandant naujiems procesams, bei plečiantis darbuotojų komandai. Sąlygose yra teigiama, jog vartotojai turi pateikti informaciją apie save, kuri bus naudojama identifikacijai, pavyzdžiui, vartotojo vardas, elektroninis paštas, mokėjimų duomenys ar kitokia informacija, kuri gali būti susieta su konkrečiu vartotoju.

Taip pat, Google sąlygose teigiama, kad yra renkama vartotojo informacija apie jo aktyvu-

mą naudojantis Google paslaugomis. Tokio tipo renkama informacija gali būti: paieškos terminai, peržiūrėti vaizdo įrašai, balso ir garso informacija naudojantis garso funkcionalumu, asmenų su kuriais vartotojas bendrauja duomenys, paieškos istorija. Ši informacija gali būti panaudota įvairiems tikslams, pavyzdžiui, programėlių rekomendacija Google Play aplikacijoje. Jeigu vartotojas naudoja Google komunikavimo paslaugas, pavyzdžiui, Google Hangouts, Google gali rinkti informaciją apie skambučių istoriją, skambintojo ir skambučio gavėjo telefono numerius, skambučių bei žinučių laiką ir datą, skambučių trukmę, bei skambučių tipus. Sąlygose teigiama, kad vartotojas gali peržiūrėti ir kontroliuoti, savo Google paskyros saugomus duomenis.

Google tvirtina, jog supranta, kad skirtingi vartotojai, gali norėti skirtingų privatumo taisyklių. Būtent dėl to, Google paskyroje vartotojai gali kontroliuoti privatumo nustatymus. Taip pat tobulėjant Google technologijom, kartu keičiasi ir privatumo nustatymai tokiu būdu užtikrinant vartotojų pasirinkimą kontroliuoti savo privatumą visais atvejais. Google teigia, jog vartotojo asmeniniai duomenys gali būti panaudoti trečių šalių marketingo organizacijų, tačiau taip pat užtikrina, kad vartotojo duomenys nėra pardavinėjami kitoms organizacijoms. Taip pat sąlygose rašoma, kad Google gali rodyti tikslinės auditorijos reklamas, tačiau vartotojai turi galimybę modifikuoti savo interesus, pasirinkti ar jų asmeninė informacija gali būti naudojama personalizuotoms reklamoms, bei įjungti arba išjungti tam tikras marketingo paslaugas. Sąlygose taip pat yra pabrėžiama, kad Google leidžia specifiniams partneriams rinkti informaciją iš vartotojų naršyklių arba įrenginių bei tuos duomenis naudoti reklamavimo tikslais, naudojant jų pačių slapukus (angl. cookies) arba kitas tokio tipo technologijas. Reklamos gali naudoti duomenis apie vartotojo lankomas internetines svetaines, paieškos terminus, vartotojo šalį ir panašią informaciją. Taip pat sąlygose teigiama, kad Google nerenka ir nenaudoja duomenų reklamavimo tikslais Google Cloud platformoje, G Suite produktuose. Sąlygose pabrėžiama, kad Google nerodo personalizuotų reklamų remiantis jautria informacija, pavyzdžiui: religija, rase ar seksualine orientacija.

Google sąlygų pakete nurodoma, kad Google gerbia vartotojų privatumą ir dėl to siekia apsaugoti duomenis, kuriuos jiems suteikia vartotojai. Google teigia, jog tam kad išlaikyti Google produktų ir paslaugų saugumą, organizacija taiko labiausiai pažengusias saugumo praktikas visame pasaulyje. Tai reiškia, kad Google nuolat stiprina saugumo technologijas, kad atrastų naujas virtualaus pasaulio grėsmes bei nuo jų apsaugotų. Tačiau sąlygose rašoma, kad duomenų apsauga priklauso ne tik nuo Google, bet ir kitų internetines paslaugas suteikiančių organizacijų. Google yra viena primųjų kompanijų, sukūrusi saugumo standartus, kuriuos daugelis naudoja šiomis dienomis. Ši organizacija taip pat toliau tobulina saugumo technologijas, kurios gali būti panaudotos kitų kompanijų. Sąlygose rašoma, kad Google dalinasi savo saugumo problemų patirtimis su įvairiomis organizacijomis - savo partneriais bei konkurentais.

Sąlygose teigiama, jog Google dažnai pertvarko informacijos rinkimo, saugojimo, apdorojimo praktikas, įskaitant ir fizinį duomenų saugumą, tam kad užkirsti kelią duomenų prieigai įgaliojimo neturintiems asmenims. Google taip pat pabrėžia, kad prieiga prie vartotojo asmeninių duomenų yra ribota Google darbuotojams, partneriams, bei asmenims, kuriems reikia informacijos, duomenų apdorojimo tikslais. Kiekvienas asmuo, turintis prieigą prie duomenų, turi pasirašyti griežtą konfidencialumo sutartį ir nesilaikius taisyklių, turi atsakyti už savo veiksmus. Atsirandant

naujiems trečiųjų šalių partneriams, Google rengia saugumo ir privatumo patikrinimą, tam kad įsitikinti ar kitos organizacijos laikosi atitinkamų saugumo principų. Taip pat sąlygose rašoma, kad norint išlaikyti vartotojo duomenų privatumą duomenų perdavimo metu bei saugant informaciją serveryje Google šifruoja duomenis. Google teigia, kad įvykus duomenų įsilaužimams, Google informuos vartotojus iškart ir sieks sumažinti vartotojų patirtą žalą kaip įmanoma labiau.

Google sąlygose yra teigiama, jog šios organizacijos teikiamos paslaugos leidžia vartotojams sąveikauti ir dalintis informacija su kitais Google patikimais ir nepatikimais vartotojais, pavyzdžiui, siųsti elektroninį laišką ne Google vartotojams. Tai reiškia, kad egzistuoja galimybė, jog vartotojo duomenys atsidurs Google nekontroliuojamoje aplinkoje, kuri neužtikrina duomenų saugumo. Jei-gu vartotojas turi Google paskyrą, jis gali paviešinti savo profilio vardą, profilio nuotrauką bei su Google sistema atliekamus veiksmus.

Google sąlygose yra pabrėžiama, kad viešinama vartotojų informacija gali būti pasiekama naudojant įvairias paieškos sistemas (angl. search engines), tarp kurių yra ir Google. Prisijungusiam prie Google paskyros vartotojui naudojantis Google paslaugomis, pavyzdžiui, komentuojant YouTube vaizdo įrašus arba rašant atsiliepimus Google Play programėlėje, bus viešai matomi vartotojo duomenys: vartotojo vardas ir nuotrauka. Tačiau taip pat sąlygose yra teigiama, jog vartotojai turi galimybę patys kontroliuoti savo kontaktinius duomenis ir pasirinkti ar jų vardas ir nuotrauka bus viešai matomi naudojantis Google paslaugomis. Taip pat Google suteikia "My Activity" funkcionalumą, kuris leidžia vartotojams peržiūrėti ir kontroliuoti duomenis, kurie yra sukuriami naudojantis Google paslaugomis. Pavyzdžiui, peržiūrėti duomenis apie vartotojo apsilankymus Google Play programėlėje arba vartotojo atliktas paieškas. Šie duomenys gali būti ieškomi pagal sukūrimo datą ir temą bei gali būti ištrinti vartotojui panorėjus.

4.3. Apple Siri privatumo įvertinimas

Šiame vertinime yra atsižvelgiama tik į viešai prieinamą informaciją apie Apple produktus. [APP22a] [APP22b] [APP22c] [APP22d] [APP22e] [APP22f] [APP22g] [APP22h] [APP22i]

Apple sąlygose yra teigiama, kad vartotojų privatumas yra viena svarbiausių žmogaus teisių ir privatumo užtikrinimo mechanizmai yra naudojami visuose Apple produktuose, aplikacijose ir paslaugose. Vartotojui susikūrus Apple ID, pradedama rinkti įvairaus tipo informacija: vartotojo vardas, elektroninis paštas, telefono numeris, įrenginio identifikavimo informacija, IP adresas, lokacijos informacija bei kreditinės kortelės informacija. Taip pat Apple teigia, kad Siri paieškos yra susietos su unikaliu indetifikatoriumi, tačiau ne Apple ID. Tai reiškia, kad asmeninė informacija nėra renkama bendrinimui su kitomis organizacijoms. Apple sąlygose taip pat rašoma, kad Siri vartotojai gali iš naujo nusistatyti identifikatorių, tokiu būdu ištrindami visą ankščiau sukaupą informaciją apie sąveiką su Siri.

Sąlygose teigiama, kad vartotojo duomenys gali būti bendrinami su trečiųjų šalių aplikacijomis tik su tikslu pagerinti Apple produktų ir teikiamų paslaugų kokybę. Asmeninė informacija nėra bendrinama kitoms organizacijoms tik dėl tų organizacijų tikslų. Tačiau Apple gali naudoti, perkelti ar atskleisti ne asmeninę informaciją bet kokiais tikslais. Tai reiškia, kad Apple svetainės, internetinės paslaugos, aplikacijos, elektroniniai laiškai ir trečiųjų šalių aplikacijų reklamavimas gali

naudoti sekimo (angl. tracking) technologijas tam, kad pagerintų Apple supratimą apie vartotojų elgesį.

Taip pat Apple suteikia vartotojams "Limit Ad Tracking" pasirinkimą, kuris užtikrina, kad vartotojas negautų tikslinės auditorijos reklamų. Galiausiai Apple sąlygose yra tvirtinama, kad ši organizacija nerenka duomenų apie vartotojus iš trečių šalių svetainių tikslinės auditorijos reklamavimo tikslams bei nepriima sprendimų susijusių su algoritmų bei profiliavimo naudojimu, kurie galėtų daryti stiprią įtaką vartotojams.

Apple sąlygose rašoma, kad saugumas ir privatumas yra pagrindinis aspektas, kuriant Apple techninę ir programinę įrangą. Apple siekia užtikrinti, kad kiekvienas vartotojo patirties aspektas būtų paremtas naujausiomis privatumo ir saugumo praktikomis. Sąlygose teigiama, jog saugant asmeninę vartotojo informaciją, Apple riboja fizinę priėjimą prie vartotojo duomenų. Taip pat Apple teigia, kad privatumo ir saugumo užtikrinimo gairės yra žinomos visiems Apple darbuotojams.

Taip pat sąlygose teigiama, kad iCloud platforma yra paremta standartiniais saugumo principais ir naudojamos griežtos taisyklės, kad apsaugoti iCloud laikomus duomenis. iCloud naudoja duomenų šifravimą siunčiant informaciją internetu bei saugant duomenis serveryje. Apple taip pat riboja priėjimą prie duomenų naudojant saugius autentifikavimo tokenus informacijos perdavimo metu bei saugant duomenis iCloud platformoje. iCloud naudoja 128 bitų AES (angl. Advanced Encryption Standard) šifravimą ir niekada nesuteikia šifravimo raktų kitoms organizacijoms. Šifravimo raktai yra laikomi Apple duomenų centruose ir Apple ID slaptažodžiai bei įgaliojamieji raštai (angl. credentials) yra saugomi iCloud duombazėse tokiu būdu, kad patys Apple negalėtų jų perskaityti ar pasiekti.

Taip pat, Apple sąlygų rinkinyje rašoma, kad dėl Apple naudojamų šifravimo metodų, vartotojai būtinai turi instaliuoti kelių faktorių autentifikaciją (angl. two-factor authentication) susietą su vartotojo Apple ID. Taip pat Apple teigia, kad nuolatinis programinės įrangos atnaujinimas ir kelių faktorių autentifikacijos naudojimas yra svarbiausios saugumo priemonės, kurias gali panaudoti vartotojai.

Apple sąlygose teigiama, kad vartotojams dalinantis informacija su kitais asmenimis, jų profilio informacija, pavyzdžiui, vartotojo vardas ar kontaktinė informacija gali būti paviešinta. Apple taip pat pabrėžia, kad informacija, kuria vartotojai dalinasi su kitais vartotojais gali būti pasiekiamas, renkama ir naudojama tų vartotojų.

4.4. Amazon Alexa privatumo įvertinimas

Šiame vertinime yra atsižvelgiama tik į viešai prieinamą informaciją apie Amazon produktus. [AMA22a] [AMA22b]

Amazon teigia, kad jų produktai renka vartotojų asmeninę informaciją dėl to nes ši informacija padeda suteikti labiau personalizuotą vartotojų patirtį bei nuolat tobulinti Amazon produktus. Pavyzdžiui, Amazon Echo Look įrenginys naudoja vartotojo nuotraukas, kad galėtų rekomenduoti vartotojui drabužius, kurie dera prie jo įprasto stiliaus pasirinkimo. Amazon sąlygose rašoma, kad ši organizacija renka duomenis tam, kad suteiktų prekinimosi galimybes, pateiktu rekomendacijas, suteiktu balsu teikiamas paslaugas, rodytų reklamas bei apsaugotų vartotojus nuo apgavysčių.

Sąlygose teigiama, kad Amazon nekontroliuoja kokius slapukus ar kitokius funkcionalumus naudoja reklamuotojai (angl. advertisers) arba kitos trečių šalių organizacijos, kurios naudoja Amazon duomenis. Taip pat duomenų saugumas ir privatumas nėra užtikrinamas kitų organizacijų.

Tačiau Amazon privatumo politikoje teigiama, kad ši organizacija siekia informuoti vartotojus apie naujų organizacijų įsitraukimą, bei mažinti duomenų bendrinimą. Taip pat rašoma, kad Amazon nesuteikia jokios vartotojo identifikavimo informacijos reklamuotojams arba kitoms trečių šalių organizacijoms, kurios vaizduoja personalizuotas reklamas. Trečių šalių kompanijos gali naudoti vartotojo duomenis tam, kad atliktų Amazon teikiamą funkciją, tačiau negali naudoti savo tikslams. Taip pat sąlygose rašoma, kad vartotojai turi galimybę pasirinkti ar jų asmeninė informacija gali būti naudojama personalizuotoms reklamoms. Amazon teigia, kad vartotojai turi galimybę patys pridėti arba pakeisti apie save saugomą informaciją. Taip pat vartotojai turi galimybę atsisakyti marketingo komunikacijų bei personalizuotų reklamų. Amazon teigia, kad vartotojai gali pasiekti apie juos saugomą informaciją, pavyzdžiui, adresą, vardą, mokėjimo informaciją, profilio informaciją, prenumeratų duomenis, pirkimų istoriją.

Amazon sąlygose yra teigiama, kad vartotojai turi galimybę, rašyti atsiliepimus, komentarus, kelti nuotraukas, vaizdo įrašus ir kitokį turinį. Sąlygose rašoma, kad ši organizaciją turi teisę, tačiau ne privalo, ištrinti arba keisti vartotojų turinį, tačiau tas turinys reguliariai nėra peržiūrimas. Taip pat sąlygose rašoma, kad Amazon saugo vartotojo žinutes naudojamas Alexa asistentui, tam kad vartotojas galėtų jas pasiekti Alexa programėleje ir kituose įrenginiuose su Alexa integracija. Taip pat Amazon pabrėžia, kad Alexa paskyros nustatymuose yra galimybė ištrinti balso įrašus.

Registruojantis prie Amazon Alexa produktų, vartotojai privalo pateikti savo telefono numerį, norint naudotis Alexa Communications funkcionalumu. Taip pat dėl saugumo tikslų, Amazon turi patvirtinti tą numerį siunčiant SMS žinutę. Sąlygų rinkinyje rašoma, kad vartotojai, kurie žino kitų vartotojų naudotojo registracijos vardą ar kitus kontaktinius duomenis, turės galimybę komunuoti naudojant Alexa Communication aplikaciją. Taip pat naudotojo telefono numeris gali būti pavaizduotas kaip skambintojo ID, skambinant kitiems vartotojams. Taip pat Amazon sąlygose yra rašoma, kad vartotojo informacija yra šifruojama duomenų perdavimo metu naudojant SSL (angl. Secure Sockets Layer) šifravimą.

4.5. Balso asistentų palyginimas

Balso asistentų palyginimas vyko nagrinėjant viešą organizacijų informaciją apie jų produktų naudojimosi sąlygas bei privatumo politiką.

4.5.1. Duomenų rinkimas

Atliekant duomenų rinkimo palyginimą tarp balso asistentų organizacijų, geriausiai pasirodė Google dėl aiškiausiai apibrėžtų taisyklių apie renkamus duomenis. Google sąlygose buvo atrasta, jog yra renkama identifikacijos, biometrinė, sveikatos, geografinės padeties informacija. Panašiai galima įvertinti ir Siri balso asistentą, tačiau dėl neaiškumo ar yra renkama jautri vartotojo informacija, Siri lieka antroje vietoje. Amazon Alexa įvertintas prasčiausiai šiuo aspektu, nes nėra pateikta

pakankamai informacijos apie duomenų rinkimą. Trūksta aiškumo ar yra renkama biometrinė informacija bei sveikatos duomenys, bei sąlygose nėra pabrėžta ar duomenys yra renkami su vartotojo sutikimu.

1. Ar renkama identifikacijos informacija?
2. Ar renkama biometrinė informacija ir sveikatos duomenys?
3. Ar renkami geografinės padėties duomenys?
4. Ar renkama jautri naudotojų informacija?
5. Ar duomenys renkami tik su vartotojo sutikimu?
6. Ar vartotojų asmeninė informacija yra renkama naudojant trečių šalių sistemas?

2 lentelė. Duomenų rinkimo palyginimas

Kriterijus	Google Assistant	Siri	Alexa
1.	Taip	Taip	Taip
2.	Taip	Taip	Nežinoma
3.	Taip	Taip	Taip
4.	Taip	Nežinoma	Taip
5.	Taip	Ne	Nežinoma
6.	Taip	Taip	Taip

Įvertinimas nuo geriausio iki prasčiausio pagal duomenų rinkimo kriterijų:

1. Google Assistant
2. Siri
3. Alexa

4.5.2. Duomenų bendrinimas

Duomenų bendrinimo aspektu visos organizacijos yra panašioje situacijoje. Visos trijų kompanijų sąlygose yra teigiama, kad jos dalinasi informacija su trečių šalių sistemomis dėl sąlygose pateiktų priežasčių, tačiau riboja bendrinamų duomenų naudojimą pagal tam tikras sutartyje pateiktas taisykles, pasirašomas su trečių šalių organizacijomis.

1. Ar renkama informacija yra bendrinama su trečių šalių sistemomis?
2. Ar nurodyti duomenų bendrinimo su trečių šalių sistemomis tikslai?
3. Ar vartotojo duomenų, bendrinamų su trečių šalių sistemomis, naudojimas yra ribotas pagal pasirašytus kontraktus su kitomis organizacijomis?

3 lentelė. Duomenų bendrinimo palyginimas

Kriterijus	Google Assistant	Siri	Alexa
1.	Taip	Taip	Taip
2.	Taip	Taip	Taip
3.	Taip	Taip	Taip

Įvertinimas nuo geriausio iki prasčiausio pagal duomenų bendrinimo kriterijų:

1. Siri, Google Assistant, Alexa

4.5.3. Duomenų apsauga

Daugiausiai informacijos apie duomenų apsaugą suteikė Google Assistant. Google suteikia kelių veiksmų autentifikavimą, ribojama darbuotojų bei fizinė prieiga prie vartotojo duomenų, duomenys yra šifruojami, užtikrinama, kad kitos organizacijos naudojančios jų duomenis taip pat laikosi aukštų saugumo standartų. Siri nepateikia pakankamai informacijos apie trečių šalių organizacijų saugumo standartų laikymąsi, bei skirtingai nei Google nėra aišku ar vartotojai yra informuojami įvykus duomenų įsilaužimams. Amazon Alexa įvertinta prasčiausiai dėl neaiškios informacijos apie kelių veiksmų autentifikacijos palaikymo, duomenų šifravimo, informavimo apie įsilaužimus bei neaiškumo dėl prieigos ribojimo prie vartotojo duomenų.

1. Ar vartotojo tapatybė yra patvirtinama su papildoma identifikavimo informacija?
2. Ar yra kelių veiksmų (angl. multi-factor) paskyros apsauga?
3. Ar trečių šalių sistemos turinčios prieigą prie vartotojo duomenų turi palaikyti tokius pačius saugumo užtikrinimo principus kaip ir pati organizacija?
4. Ar darbuotojų prieiga prie duomenų yra ribota?
5. Ar fizinis duomenų prieinamumas yra ribotas?
6. Ar duomenų perdavimo metu informacija yra užšifruota?
7. Ar saugomi duomenys yra užšifruoti?
8. Ar organizacija informuoja vartotojus apie įvykusius duomenų įsilaužimus?

4 lentelė. Duomenų apsaugos palyginimas

Kriterijus	Google Assistant	Siri	Alexa
1.	Taip	Taip	Taip
2.	Taip	Taip	Nežinoma
3.	Taip	Nežinoma	Taip
4.	Taip	Taip	Nežinoma
5.	Taip	Taip	Nežinoma
6.	Taip	Taip	Taip
7.	Taip	Taip	Nežinoma
8.	Taip	Nežinoma	Nežinoma

Įvertinimas nuo geriausio iki prasčiausio pagal duomenų apsaugos kriterijų:

1. Google Assistant
2. Siri
3. Alexa

4.5.4. Duomenų teisės

Duomenų teisių aspektu tiek Google Assistant tiek Siri buvo įvertinti vienodai gerai. Abi organizacijos teigia, kad vartotojai turi teisę į savo asmeninius duomenis, turi galimybę pasiekti apie juos saugomus duomenis, juos keisti bei ištrinti, ištrynus vartotojo paskyrą taip pat yra ištrinami ir vartotojo duomenys, taip pat yra ištrinami nebenaudojami vartotojo duomenys, prieiga prie duomenų yra ribojama, bei egzistuoja galimybė duomenis parsisiųsti. Alexa neturi tiek daug privalumų

nes trūksta informacijos apie vartotojo nuosavybės teisę į apie jį saugomus duomenis, duomenų ištrinimą, bei galimybes parsisiųsti saugomą informaciją.

1. Ar vartotojai turi nuosavybės teisę į savo asmeninius duomenis?
2. Ar vartotojai turi galimybę pasiekti ir peržiūrėti apie juos saugomus duomenis?
3. Ar vartotojai turi galimybę keisti apie juos saugomus duomenis?
4. Ar vartotojai turi galimybę ištrinti apie juos saugomus duomenis?
5. Ar ištrynus naudotojo paskyra, kartu yra ištrinami ir jo duomenys?
6. Ar duomenys yra ištrinami kai jie nebėra naudojami?
7. Ar yra galimybė vartotojui parsisiųsti savo asmeninę informaciją?

5 lentelė. Duomenų teisių palyginimas

Kriterijus	Google Assistant	Siri	Alexa
1.	Taip	Taip	Nežinoma
2.	Taip	Taip	Taip
3.	Taip	Taip	Taip
4.	Taip	Taip	Taip
5.	Taip	Taip	Nežinoma
6.	Taip	Taip	Nežinoma
7.	Taip	Taip	Nežinoma

Įvertinimas nuo geriausio iki prasčiausio pagal duomenų teisių kriterijų:

1. Google Assistant, Siri
2. Alexa

4.5.5. Vartotojo kontrolė

Kontrolės aspektu Google Assistant buvo įvertintas geriausiai. Sąlygose teigiama, kad Google Assistant naudotojai gali kontroliuoti apie juos renkama informaciją naudojant privatumo nustatymus, renkama informacija naudojama tik sąlygose apibrėžtais tikslais, organizacija gali sujungti duomenis su kita informacija gauta iš trečių šalių šaltinių bei tokia kombinuota informacija yra vis tiek laikoma identifikacijos informacija, vartotojams pranešama apie duomenų rinkimo pokyčius bei yra prašomas vartotojų sutikimas, vartotojams suteikiama informacija apie jų asmeninių duomenų bendrinimą, ir vartotojams pranešama jeigu teisinės institucijos pareikalauja jų duomenų. Apple nesuteikė tiek informacijos šiuo aspektu. Sąlygose nebuvo aišku ar vartotojai informuojami bei prašomas naujas sutikimas pasikeitus duomenų rinkimo sąlygom. Tiek Amazon tiek Apple nepateikia informacijos ar yra galimybė vartotojams gauti su kitomis organizacijomis bendrinamą informaciją. Taip pat Amazon sąlygose nėra aišku ar kombinuota vartotojo informacija yra laikoma identifikacijos informacija, bei Amazon teigia, kad vartotojams nėra pranešama jeigu teisinės institucijos pareikalauja jų duomenų.

1. Ar vartotojai gali kontroliuoti apie juos renkama informaciją naudojant privatumo nustatymus?
2. Ar naudotojai gali atsisakyti atskleisti savo duomenis kitoms organizacijoms?

3. Ar informacija yra panaudojama tik tiems tikslams dėl kurių ji buvo rinkta?
4. Ar organizacija gali sujungti duomenis su papildoma informacija iš trečių šalių šaltinių?
5. Ar kombinuota informacija yra laikoma identifikacijos informacija?
6. Ar vartotojams pranešama jeigu pasikeičia priežastis dėl kurios duomenys yra renkami?
7. Ar organizacija prašo vartotojų iš naujo sutikti su sąlygomis ir taisyklėmis jeigu pasikeičia duomenų surinkimo praktikos?
8. Ar vartotojai gali paprašyti gauti su kitom organizacijom bendrinamą asmeninę informaciją?
9. Ar vartotojui pranešama jeigu jo duomenų pareikalauja vyriausybė arba kitos teisinės institucijos?

6 lentelė. Vartotojo kontrolės palyginimas

Kriterijus	Google Assistant	Siri	Alexa
1.	Taip	Taip	Taip
2.	Taip	Taip	Taip
3.	Taip	Taip	Ne
4.	Taip	Taip	Taip
5.	Taip	Taip	Nežinoma
6.	Taip	Nežinoma	Taip
7.	Taip	Nežinoma	Taip
8.	Taip	Nežinoma	Nežinoma
9.	Taip	Taip	Ne

Įvertinimas nuo geriausio iki prasčiausio pagal duomenų teisių kriterijų:

1. Google Assistant
2. Siri, Alexa

4.5.6. Duomenų pardavinėjimas

Šiuo aspektu visos trys organizacijos teigia, kad nepardavinėja vartotojo duomenų trečių šalių organizacijoms, suteikia naudotojams galimybę atsisakyti atskleisti duomenis kitoms organizacijoms, vartotojo duomenys gali būti perduoti kitoms kompanijoms įvykus organizacijų susijungimui, įsigyjant naują kompaniją arba bankroto atveju. Taip pat nėra aišku ar tiriamos organizacijos duoda galimybę vartotojams ištrinti asmeninę informaciją prieš įvykstant duomenų perdavimui. Informacija apie vartotojų informavimą įvykus duomenų perdavimui pateikiama tik Google sąlygose. Taip pat, tiek Google tiek Apple bendrina duomenis anonimišku formatu, tačiau nėra aišku kokiais būdais tie duomenys anonimizuojami. Trečių šalių organizacijų duomenų identifikavimas yra draudžiamas tik Apple. Šiuo aspektu tiek Amazon Alexa suteikia mažiausiai informacijos.

1. Ar vartotojų asmeniniai duomenys nėra pardavinėjami trečių šalių organizacijoms?
2. Ar vartotojų duomenys gali būti perduoti trečių šalių organizacijoms vykstant organizacijų susijungimams, įsigyjant naują kompaniją arba bankroto atveju?
3. Ar naudotojai yra informuoti įvykus duomenų perdavimui kitai organizacijai?
4. Ar vartotojai gali ištrinti savo informaciją prieš perduodant ją kitai organizacijai?
5. Ar vartotojų duomenys yra bendrinami anonimišku formatu?

6. Ar organizacija atskleidžia kokiais būdais anonimizuojami vartotojo duomenys?
7. Ar organizacija draudžia trečių šalių organizacijoms identifikuoti duomenis?

7 lentelė. Duomenų pardavinėjimo palyginimas

Kriterijus	Google Assistant	Siri	Alexa
1.	Taip	Taip	Taip
2.	Taip	Taip	Taip
3.	Taip	Nežinoma	Nežinoma
4.	Nežinoma	Nežinoma	Nežinoma
5.	Taip	Taip	Nežinoma
6.	Nežinoma	Nežinoma	Nežinoma
7.	Nežinoma	Taip	Nežinoma

Įvertinimas nuo geriausio iki prasčiausio pagal duomenų pardavinėjimo kriterijų:

1. Google Assistant, Siri
2. Alexa

4.5.7. Produkto apsauga

Produkto apsaugos aspektu Siri įvertintas geriausiai, antroje vietoje Google Assistant, trečioje Alexa. Visų organizacijų sąlygose buvo rašoma, kad vartotojai gali sąveikauti su nepatikimais asmenimis bei naudotojų profilio informacija yra bendrinama norint komunikuoti su kitais vartotojais. Siri balso asistentas vienintelis nereikalauja viešinti asmeninės informacijos. Taip pat Google ir Apple suteikia vartotojams galimybę kontroliuoti jų asmeninės informacijos vaizdavimą kitiems vartotojams, tačiau ši informacija nežinoma apie Amazon produktus. Amazon yra vienintelė iš trijų organizacijų, kuri neperžiūri ir neįvertina vartotojo kuriamo turinio. Taip pat Amazon nefiltruoja asmeninės informacijos esančios vartotojo sukurtam turinį. Ši informacija nėra pateikta Apple ir Google sąlygose. Apple priešingai nei Amazon ir Google nesuteikia informacijos apie sąveiką tarp vartotojų duomenų rinkimą.

1. Ar vartotojai gali sąveikauti su nepatikimais vartotojais?
2. Ar profilio informacija turi būti bendrinama norint socializuotis su kitais vartotojais?
3. Ar asmeninė informacija turi būti rodoma viešai?
4. Ar vartotojai gali kontroliuoti kokia informacija yra atvaizduojama kitiems vartotojams?
5. Ar vartotojų sukurtas turinys yra peržiūrimas ir įvertinimas?
6. Ar vartotojų sukurtas turinys, turintis asmeninės informacijos, yra išfiltruojamas prieš jį paviešinant?
7. Ar yra renkami duomenys apie sąveikas tarp vartotojų?

8 lentelė. Produktų apsaugos palyginimas

Kriterijus	Google Assistant	Siri	Alexa
1.	Taip	Taip	Taip
2.	Taip	Taip	Taip
3.	Taip	Ne	Taip
4.	Taip	Taip	Nežinoma
5.	Taip	Taip	Ne
6.	Nežinoma	Nežinoma	Ne
7.	Taip	Nežinoma	Taip

Įvertinimas nuo geriausio iki prasčiausio pagal produkto apsaugos kriterijų:

1. Siri
2. Google Assistant
3. Alexa

4.5.8. Reklamos ir duomenų stebėjimas

Šiuo aspektu Siri įvertintas geriausiai, antroje vietoje Alexa ir Google Assistant. Apple sąlygose teigiama, jog vartotojo asmeninė informacija nėra bendrinama su trečių šalių marketingo organizacijomis, nėra kuriami vartotojų duomenų profiliai skirti personalizuotoms reklamoms, vartotojo informacija nėra naudojama reklamoms kitose trečių šalių sistemose. Visi šie aspektai buvo įvertinti priešingai Google ir Amazon organizacijose. Visos trys organizacijos leidžia vartotojams atsisakyti personalizuotų reklamų bei Apple nepateikia jokios informacijos apie marketingo komunikacijos atsisakymo.

1. Ar asmeninė informacija yra bendrinama trečių šalių marketingo organizacijoms?
2. Ar kuriami duomenų profiliai skirti personalizuotoms reklamoms?
3. Ar vartotojo informacija nėra naudojama reklamoms kitose trečių šalių sistemose?
4. Ar vartotojai gali atsisakyti personalizuotų reklamų?
5. Ar vartotojai gali atsisakyti marketingo komunikacijos?

9 lentelė. Reklamos ir duomenų stebėjimo palyginimas

Kriterijus	Google Assistant	Siri	Alexa
1.	Taip	Ne	Taip
2.	Taip	Ne	Taip
3.	Taip	Ne	Taip
4.	Taip	Taip	Taip
5.	Taip	Nežinoma	Taip

1. Siri
2. Google Assistant, Alexa

Rezultatai

1. Išanalizuota literatūra susijusi su balso asistentų veikimo principu, jų panašumais bei skirtumais.
2. Išanalizuota literatūra susijusi su balso asistentų keliamom privatumo problemom, vartotojų susirūpinimu privatumo klausimais, privatumo įtaka pasitikėjimu organizacijomis, privatumo užtikrinimo reglamentu - BDAR.
3. Sukurtas privatumo kriterijų rinkinys skirtas įvertinti balso asistentų technologijų privatumo užtikrinimo lygį.
4. Atliktas Google Assistant, Siri ir Alexa balso asistentų palyginimas pagal sukurtą privatumo kriterijų rinkinį.

Išvados

Balso asistentai yra greitai tobulėjanti bei sparčiai pritaikoma technologija. Tačiau nors ir ši technologija vartotojams suteikia daug patogumų bei naujų galimybių automatizuoti įprastus gyvenimo procesus, balso asistentų organizacijų renkami dideli informacijos kiekiai atveria galimybes kenkėjiškiems asmenims ar asmenų grupėms išnaudoti šią technologiją vartotojams nepalankiais tikslais. Šis faktas bei praeityje įvykę vartotojų duomenų paviešinimai sukelia privatumo susirūpinimų bei mažina pasitikėjimą balso asistentų organizacijomis.

Šiame darbe buvo išnagrinėtas balso asistentų veikimo principas, vienu populiariausių balso asistentų, Google Assistant, Apple Siri ir Amazon Alexa panašumai ir skirtumai. Tarp skirtumų matome, kad skirtingi balso asistentai suteikia skirtingo tikslumo atsakymus, yra palaikomi ant skirtingų kiekių įrenginių, bei turi savitus pranašumus naudojant balso asistentus su tos pačios kompanijos kuriamais produktais. Google Assistant suteikia geriausią tikslumą, Alexa yra pritaikytas didžiausiam skirtingų įrenginių kiekiui, o Siri yra plačiausiai naudojamas asistentas. Tačiau nors šie balso asistentai buvo palyginti pagal naudojimo, pritaikymo bei patogumo aspektais, nagrinėjant literatūra buvo pasigesta informacijos apie šių technologijų privatumo palyginimą. Taigi šiame darbe buvo atliktas tyrimas skirtas palyginti populiariausių balso asistentų privatumo užtikrinimą.

Šis įvertinimas buvo atliktas palyginimo principu, sukuriant kriterijų rinkinį ir atliekant lyginamąją analizę tarp Google, Amazon ir Apple kuriamų balso asistento technologijų. Kriterijų rinkinys buvo kuriamas išnagrinėjant vartotojų susirūpinimus privatumo klausimais, įvertinant privatumo problemų įtaką organizacijų pasitikėjimui bei pažvelgiant į BDAR reglamento punktus, kurie yra aktualūs tokioms technologijoms kaip balso asistentai.

Atlikus šį palyginimą matosi, kad daugiausiai kartų aukščiausią įvertinimą gavo Google Assistant ir dėl to galime teikti, jog Google yra labiausiai privatumą užtikrinanti organizacija, dėl didelio aiškumo apie vartotojų duomenų rinkimą, aukščiausio lygio duomenų apsaugos, bei suteikiamos duomenų valdymo kontrolės pačiam vartotojui. Siri balso asistento bendras įvertinimas yra prastesnis negu Google Assistant, tačiau Apple ryškiausias pranašumas yra vartotojo asmeninės informacijos nenaudojimas trečių šalių marketingo tikslais. Galiausiai Amazon Alexa balso asistentas yra įvertintas prasčiausiai beveik visuose aspektuose, dėl mažiausiai suteikiamos informacijos apie vartotojų privatumą bei duomenų apsaugą. Tačiau nepaisant gero Google Assistant balso asistento įvertinimo privatumo klausimais, šis tyrimas neužtikrina, kad vartotojai naudojantys Google Assistant nesusidurs su privatumo problemomis. Šio tyrimo rezultatai gali padėti nuspręsti kurį balso asistentą verta rinktis naudoti labiau, tačiau vartotojai vertinantys savo duomenų privatumą turėtų vis tiek būti atsargūs, bei suprasti, kad naudojantis visais trim balso asistentais bus renkami jų asmeniniai duomenys ir egzistuoja rizika, kad tie duomenys pateks į blogas rankas.

Literatūra

- [LAR22] Number of digital voice assistants in use worldwide 2019-2024. Prieiga per internetą: <https://www.statista.com/statistics/973815/worldwide-digital-voice-assistant-in-use/>
- [RWL+18] Comparing Speech and Keyboard Text Entry for Short Messages in Two Languages on Touchscreen Phones. 2018. Prieiga internetu: <https://dl.acm.org/doi/abs/10.1145/3161187>
- [WOL18] Sam Wolfson. 2018. Amazon's Alexa recorded private conversation and sent it to random contact. Prieiga per internetą: <https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation>
- [STE22] A quick and easy guide to voice assistants. Prieiga per internetą: <https://www.miquido.com/blog/what-are-voice-assistants/>
- [TIL22] What is Google Assistant and what can it do? Prieiga per internetą: <https://www.pocket-lint.com/apps/news/google/137722-what-is-google-assistant-how-does-it-work-and-which-devices-offer-it>
- [OBO21] What is Siri and how does Siri work? Prieiga per internetą: <https://www.pocket-lint.com/apps/news/apple/112346-what-is-siri-apple-s-personal-voice-assistant-explained>
- [RUT22] Amazon Alexa: Everything you need to know about the digital assistant. Prieiga per internetą: <https://www.androidauthority.com/amazon-alexa-878058/>
- [LVK+19] Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption. 2019. Prieiga internetu: https://link.springer.com/chapter/10.1007/978-3-030-15742-5_9.
- [SCA18] Voice recognition (speaker recognition). Prieiga per internetą: <https://www.techtarget.com/searchcustomerexperience/definition/voice-recognition-speaker-recognition>.
- [BUI21] What is Artificial Intelligence? How Does AI Work? Prieiga per internetą: <https://builtin.com/artificial-intelligence>.
- [IBM20] What is Machine Learning? Prieiga per internetą: <https://www.ibm.com/cloud/learn/machine-learning>.
- [KFA+17] What your voice says about you: Automatic Speaker Profiling using i-vectors. 2017. Prieiga internetu: http://3.9.85.185/wp-content/uploads/2019/03/IAFPA17_SpeakerProfiling_Kelly_et_al.pdf

- [SHU15] When your voice betrays you. Prieiga per internetą: <https://www.science.org/doi/full/10.1126/science.347.6221.494..>
- [EUR18] European Commission. 2018 Reform of EU Data Protection Rules. Prieiga internetu: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_lt.
- [HSP+18] Streaming end-to-end speech recognition for mobile devices. 2018. Prieiga internetu: <https://arxiv.org/pdf/1811.06621.pdf?fbclid=IwAR3Ya9ZfBNN40U00wct7dGupjlBFEPu47IRHK-wXmejI4U2UQGf03sXHMLw.I>.
- [BFR+18] VoiceGuard: Secure and Private Speech Processing. 2018. Prieiga internetu: https://www.isca-speech.org/archive/pdfs/interspeech_2018/brasser18_interspeech.pdf.
- [KUM18] Big Data Facts. 2018. Prieiga internetu: <https://analyticsweek.com/big-data-facts/>.
- [GCM16] On the track of Artificial Intelligence: Learning with Intelligent Personal Assistants. 2016. Prieiga internetu: <https://www.j-humansciences.com/ojs/index.php/IJHS/article/view/3549>.
- [RST16] A review of Internet of Things for smart home: challenges and solutions. Prieiga internetu: https://iotiran.com/wp-content/uploads/2021/02/A_review_of_Internet_of_Things_for_smart_home_Challenges_and_solutions.pdf
- [KBL+16] Who Owns the Data? Open Data for Healthcare. 2016. Prieiga internetu: frontiersin.org/articles/10.3389/fpubh.2016.00007/full.
- [DWK15] A view on privacy and trust in IoT. 2015. Prieiga internetu: <https://ieeexplore.ieee.org/document/7247581>.
- [SZK+17] Security and Trusted Devices in the Context of Internet of Things. 2017. Prieiga internetu: <https://ieeexplore.ieee.org/document/8049831>.
- [GRA17] Amazon's Alexa can now update you on your Fitbit progress. 2017. Prieiga internetu: <https://www.cnet.com/tech/mobile/amazons-alexa-fitbit-integration/>.
- [WMS16] The Extreme Risk of Personal Data Breaches and The Erosion of Privacy. Prieiga internetu: <https://arxiv.org/abs/1505.07684>.
- [AND17] Alexa, Understand Me. 2017. Prieiga internetu: <https://www.technologyreview.com/2017/08/09/149815/alexa-understand-me/>.
- [RPP+18] Using intelligent personal assistants to assist the elderlies An evaluation of Amazon Alexa, Google Assistant, Microsoft Cortana, and Apple Siri. 2018. Prieiga internetu: <https://ieeexplore.ieee.org/abstract/document/8559503>.

- [JAO18] A study of security and privacy issues associated with the Amazon Echo. 2018. Prieiga internetu: <https://www.inderscienceonline.com/doi/abs/10.1504/IJITCA.2018.090172>.
- [TOK+17] Intelligent (Smart) E-Commerce. 2017. Prieiga internetu: https://link.springer.com/chapter/10.1007/978-3-319-58715-8_7.
- [WSK+18] Speaker Recognition Using Convolutional Neural Network with Minimal Training Data for Smart Home Solutions. 2018. Prieiga internetu: <https://ieeexplore.ieee.org/abstract/document/8431363>.
- [HPA17] The new General Data Protection Regulation: Still a sound system for the protection of individuals? 2017. Prieiga internetu: <https://www.sciencedirect.com/science/article/abs/pii/S0267364916300346>.
- [GRE17] A Hacker Turned an Amazon Echo Into a 'Wiretap'. 2017. Prieiga internetu: <https://www.wired.com/story/amazon-echo-wiretap-hack/>.
- [LZS18] Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. 2018. Prieiga internetu: <https://www.key4biz.it/wp-content/uploads/2018/11/cscw102-lau-1.pdf>.
- [GOO22a] Our privacy and security principles. Prieiga internetu: <https://safety.google/principles/>.
- [GOO22b] Google Store Sales Terms. Prieiga internetu: https://store.google.com/intl/en-US_us/about/device-terms/.
- [GOO22c] Google Workspace and Cloud Identity Subprocessors. Prieiga internetu: <https://workspace.google.com/intl/en/terms/subprocessors.html>.
- [GOO22d] Google Payments Privacy Notice. Prieiga internetu: https://payments.google.com/payments/apis-secure/u/0/get_legal_document?ldo=0&ldt=privacynotice.
- [GOO22e] Google Privacy and Terms. Prieiga internetu: <https://policies.google.com/>.
- [GOO22f] Export your organization's data. Prieiga internetu: <https://support.google.com/a/answer/100458?hl=en>.
- [GOO22g] Google Cloud Privacy. Prieiga internetu: <https://support.google.com/googlecloud/answer/6056650?hl=en>.
- [GOO22h] Google Cloud Security. Prieiga internetu: <https://support.google.com/googlecloud/answer/6056693?hl=en>.
- [APP22a] Apple Privacy Policy. Prieiga internetu: <https://www.apple.com/legal/privacy/en-ww/>

- [APP22b] Apple Website Terms of Use. Prieiga internetu: <https://www.apple.com/legal/internet-services/terms/site.html>
- [APP22c] Privacy principles. Prieiga internetu: <https://www.apple.com/privacy/>
- [APP22d] Approach to privacy. Prieiga internetu: <https://www.apple.com/privacy/features/>
- [APP22e] Apple Media Services Terms and Conditions. Prieiga internetu: <https://www.apple.com/legal/internet-services/itunes/us/terms.html>
- [APP22f] iCloud Terms and Conditions. Prieiga internetu: <https://www.apple.com/legal/internet-services/icloud/en/terms.html>
- [APP22g] iCloud security overview. Prieiga internetu: <https://support.apple.com/en-us/HT202303>
- [APP22h] Apple security guide. Prieiga internetu: <https://support.apple.com/guide/security/welcome/web>
- [APP22i] Apple's Use of Cookies. Prieiga internetu: <https://www.apple.com/legal/privacy/en-ww/cookies/>
- [AMA22a] Amazon Privacy Notice. Prieiga internetu: <https://www.amazon.com/gp/help/customer/display.html?nodeId=468496>
- [AMA22b] Amazon Conditions of Use. Prieiga internetu: https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201909000
- [SRD2022] Leading devices used with voice assistants in the United States in 2021, by brand. Prieiga internetu: <https://www.statista.com/statistics/1274398/voice-assistant-use-by-device-united-states/#:~:text=A%202021%20survey%20carried%20out,voice%20assistant%20service%20of%20Apple.>
- [REW21] The best voice assistant. 2021. Prieiga internetu: <https://www.zdnet.com/home-and-office/smart-home/the-best-voice-assistant/>
- [ALH18] Improving IoT Technology Adoption through Improving Consumer Trust. 2018. Prieiga internetu: <https://www.mdpi.com/2227-7080/6/3/64>
- [CCJ18] Consumer security behaviors and trust following a data breach. 2018. Prieiga internetu: <https://www.emerald.com/insight/content/doi/10.1108/MAJ-11-2017-1692/full/html>
- [PFL19] "Phantom Friend" or "Just a Box with Information": Personification and Ontological Categorization of Smart Speaker-based Voice Assistants by Older Adults. 2019. Prieiga internetu: <https://dl.acm.org/doi/abs/10.1145/3359316>

[CLO22] Sources of big data: Where does it come from? Prieiga Internetu:
[https://www.cloudmoyo.com/blog/data-architecture/
what-is-big-data-and-where-it-comes-from/](https://www.cloudmoyo.com/blog/data-architecture/what-is-big-data-and-where-it-comes-from/)

[EUC22] What personal data is considered sensitive? Prieiga internetu:
[https://ec.europa.eu/info/law/law-topic/data-protection/reform/
rules-business-and-organisations/legal-grounds-processing-data/
sensitive-data/what-personal-data-considered-sensitive_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en)

.

Santrumpos ir sąvokų apibrėžimai

Dirbtinis intelektas (angl. Artificial intelligence) - Dirbtinis intelektas yra mašinos sugebėjimas parodyti į žmogų panašias galimybes, tokias kaip argumentavimas, mokymasis, planavimas ir kūrybiškumas.

Balso sintezė (angl. voice synthesis) - Tai kompiuterio sugeneruota žmogaus kalbos simuliacija, skirta paversti tekstą į garsą.

Kompiuterinė lingvistika (angl. computational linguistics) - lingvistikos sritis, kuri pritaiko kompiuterių mokslą kalbos analizavimui bei sintezei.

RAM atmintis (angl. Random Access Memory) - kompiuterio darbinė atmintis.

Interneto daiktai (IoT angl. Internet of Things) - tai įrenginiai turintys sensorius, duomenų apdorojimo galimybes, programinę įrangą, bei kitas integruotas technologijas kurios internetu dalinasi duomenimis su kitais įrenginiais.

Debesų sistemos (angl. Cloud-based systems) - tai galimybė naudotis kompiuterine ir programine įrangos resursais internete.

Modelio atpažinimas (angl. Pattern recognition) - tai duomenų analizavimo būdas naudojant mašininio mokymo algoritmus skirtas automatiškai atpažinti modelius ir pasikartojimus.

Mašininis mokymasis (angl. Machine learning) - dirbtinio intelekto metodų klasė, kuriai būdingas ne tiesioginis problemos sprendimas, o mokymasis, kaip pritaikyti daugelio panašių problemų sprendimus.

Biometriniai duomenys - konkretūs požymiai, pagal kuriuos galima nustatyti unikalios žmogaus savybes, tokias kaip piršto atspaudas, akies rainelė, balsas, kuriais remiantis galime patvirtinti žmogaus tapatybę.

Autentifikavimas - Autentifikavimas tikrina tai, kas yra susieta ir valdoma paties subjekto (pavyzdžiui, slaptažodžiai, skaičių žetonai), ir užtikrina, kad subjektas tai gali įrodyti.

Asmeninė identifikacijos informacija - tai informacija naudojamą atpažinti (identifikuoti) asmens tapatybę.

Asmeninė sveikatos informacija - tai informacija susijusi su asmens sveikatos būkle.

Neuroniniai tinklai - tarpusavyje sujungtų dirbtinių neuronų grupė. Ši technologija mėgdžioja žmogaus galvos smegenų darbą – tiksliau neuronų veikimą.

Profiliavimas - Profiliavimu yra laikomas toks asmenų duomenų tvarkymas, kai jie naudojami siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius asmeninius aspektus, pavyzdžiui, pomėgius, interesus, darbo rezultatus, ekonominę situaciją.

Tikslinės auditorijos reklamavimas arba personalizuotas reklamavimas (angl. targeting advertising) - tai tokia reklamavimo forma, kai reklamos yra orientuotos į tam tikrą žmonių grupę pagal asmeninę tos grupės žmonių informaciją, pavyzdžiui, vartotojų amžių, rasę, pomėgius ar politinį požiūrį.

Kelių veiksmų autentifikavimas (angl. multi-factor authentication) - yra papildomas internetinių paskyrų apsaugos lygis. Kai jis įjungtas, vartotojas turi įvesti slaptažodį ir leisti prisijungti naudodami specialią programėlę, tam tikrą laiką veikiantį kodą arba antrą prietaisą.

Duomenų šifravimas (angl. Data encryption) - tai būdas atvirą informaciją paversti uždara ir atvirkščiai.

Duomenų anonimizavimas - tai yra duomenų apdorojimo technologija, kurią taikant asmens identifikavimo informacija pašalinama arba pakeičiama; todėl anonimizuoti duomenys negali būti susieti su jokia asmeniu.

SSL (angl Secure Socket Layer) - kriptografinis protokolas, skirtas internete perduodamos informacijos apsaugai šifruojant.

Slapukas (angl. cookie) - mažas tekstinis dokumentas, turintis unikalų identifikacijos numerį, kuris yra perduodamas iš interneto tinklalapio į lankytojo kompiuterio kietąjį diską, kad tinklalapio administratorius galėtų atskirti lankytojo kompiuterį ir matyti jo veiklą internete.