BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Objek penelitian yang diambil oleh penulis dalam skripsi ini adalah adalah pengguna *Smartphone* Apple (iOS).

Gambar 1.1
Logo Apple
Sumber: www.kompasiana.com

Apple Inc adalah perusahaan teknologi multinasional asal Amerika yang berkantor pusat di Cupertino, California, Amerika Serikat. Perusahaan ini berfokus pada bidang desain, pengembangan, dan menjual produk elektronik, perangkat lunak komputer, dan layanan *online*. Apple juga membuat produk perangkat keras seperti ponsel pintar iPhone, tablet iPad, komputer Mac, Ipod portable media player, serta jam pintar Apple (*smartwatch*). Perangkat lunak yang berhasil dibuat oleh Apple ada berbagai macam, termasuk di antaranya yaitu sistem operasi komputer OS X dan sistem operasi iOS, iTunes media player, Browser web Safari, iLife dan iWork kreativitas dan produktivitas suite. Selain perangkat lunak, layanan *online* mereka meliputi iTunes Store, iOS App Store dan Mac App Store, hingga iCloud.

Perusahaan Apple sendiri di didirikan oleh Steve Jobs, Steve Wozniak dan Ronald Wayne pada tanggal 1 April 1976. Pada awalnya, perusahaan Apple bermulai di garasi rumah Steve Jobs dengan perlengkapan seadanya. Misi mereka dalam membangun komputer Apple pertama adalah untuk mengubah sudut

pandang masyarakat mengenai komputer, dimana mereka ingin membangun komputer yang cukup kecil dan *user-friendly* supaya dapat ditempatkan di rumah ataupun kantor dengan mudah. Saat itu, perusahaan Apple hanya berfokus dalam bidang mengembangkan dan menjual komputer pribadi. Diawal pendiriannya perusahaan ini bernama Apple Computer, Inc. Kemudian perusahaan ini mengganti namanya yang semula Apple Computer, Inc menjadi Apple Inc pada tanggal 3 Januari 1977. Pada tanggal 9 Januari 2007, Apple sadar untuk mulai memfokuskan diri bergeser ke arah produk elektronik (Rahim, 2016).

Apple memiliki beberapa perangkat lunak yang mereka ciptakan sendiri diantaranya adalah perangkat lunak iOS. iOS merupkan sistem operasi mobile yang dikembangkan oleh Apple dan hanya berjalan pada perangkat mobile besutan Apple yaitu iPhone, iPad, dan iPod. Pada awalnya iOS memiliki nama yang berbeda, yaitu iPhone OS. Versi pertamanya diumumkan bersamaan dengan iPhone orisinil pada 9 Januari 2007. Steve Jobs pada saat itu menjelaskan bahwa iPhone OS mengambil OS X milik perangkat Mac sebagai dasarnya. Versi perdana iPhone OS ini tidak dilengkapi App Store, semua aplikasi yang tersedia hanya buatan dari Apple sendiri. Kemudian di iPhone OS 2, bersamaan dengan diluncurkannya iPhone 3G pada tanggal 11 Juli 2008, Apple menghadirkan dukungan aplikasi pihak ketiga beserta App Store.

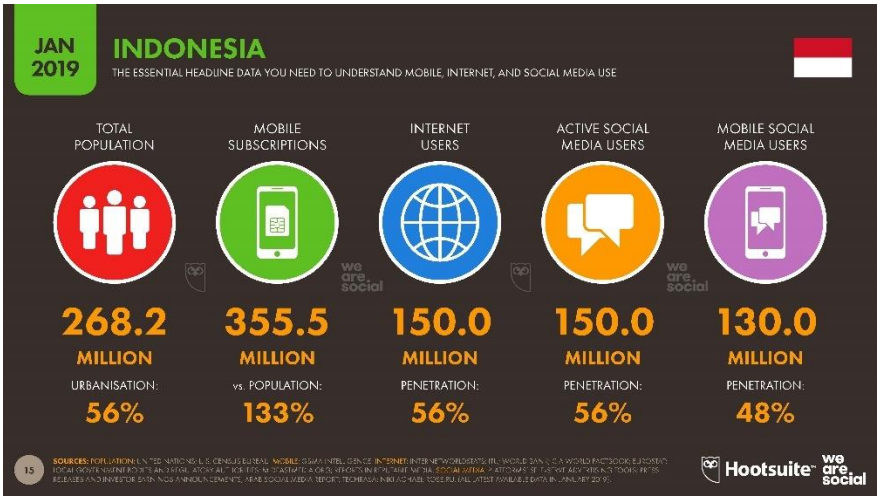
Pada tanggal 17 Juni 2009, Apple merilis iPhone OS 3 bersama dengan iPhone 3GS. Fitur baru yang paling dikenang dari versi ini adalah dukungan *copy–paste*. iPhone OS 3 juga bertanggung jawab atas tersedianya fitur *in-app purchase* (transaksi di dalam aplikasi) untuk pertama kalinya. Kemudian pada tanggal 21 Juni 2010 bersamaan dengan diumumkannya iPhone 4, iPhone OS akhirnya berganti nama menjadi iOS 4, hal ini didasari oleh penjelasan Apple bahwa sistem operasi tersebut tak hanya tersedia untuk iPhone saja, tetapi juga iPod Touch – plus iPad orisinil yang menyusul di tahun yang sama. Dalam versi ini, fitur baru yang paling berkesan adalah dukungan multitasking.

Pada dasarnya iOS merupakan sistem operasi mobile mirip seperti Android, sehingga dapat kita simpulkan bahwa system terebut merupakan nyawa dari sebuah perangkat. Secara fungsi keduanya memiliki kemiripan, akan tetapi cara kerjanya

sangatlah berbeda. Salah satu contohnya adalah di Android terdapat istilah *launcher* aplikasi sedangkan di iOS tidak, semua icon aplikasi yang terdapat di iOS akan ditampilkan di layar utama (*homescreen*). Kemudian perdeaan selanjutnya adalah Android dikembangkan dengan konsep *open-source*, sedangkan iOS dikembangkan secara tertutup oleh Apple sendiri, tanpa campur tangan dari luar. Sejak tahun 2011 setiap tahunnya Apple secara bertahap melakukan pembaharuan untuk meningkatkan kinerja pada system operasi, menambah fitur baru, dan memperbaiki kekurangan pada versi sebelumnya. Setiap versi yang dirilis disesuaikan dengan angka perilisan sebelumnya seperti iOS 5 rilis pada tahun 2011, iOS 6 rilis pada tahun 2012, iOS 7 rilis pada tahun 2013 dan seterusnya sampai dengan versi terbaru saat ini yaitu iOS 12 yang rilis pada tahun 2018 dengan kelebihan dan fitur unggalan yang dibawa (Kaonang, 2016).

1.2 Latar Belakang

Pada perkembangan saat ini, *smartphone* menjadi salah satu kebutuhan untuk bisa berkomunikasi dan berbagi informasi seperti mengirim SMS atau *email*, *entertainment*, media sosial tanpa mengkhawatirkan jarak dan waktu. Berbagai jenis *smartphone* dengan kelebihan OS (*Operating System*) nya masing-masing telah digunakan oleh setiap orang di seluruh dunia. Di Indonesia sendiri pengguna dari *smartphone* semakin meningkat setiap tahunnya sejak 2013-2018. Seperti yang dilansir dari website techinasia yang bersumber dari survei lembaga riset digital marketing Emarketer, Indonesia telah melampaui 100 juta pengguna *smartphone* aktif pada tahun 2018 dan menjadikannya negara dengan populasi pengguna *smartphone* terbesar keempat di dunia setelah China, India, dan Amerika (Millward, 2014). Sumber berita lain seperti yang dilansir dari berita websindo.com yang mengutip data dari Hootsuite mengenai hasil survey Digital Indonesia Januari 2019, menunjukan bahwa total Penduduk Indonesia mencapai 268.2 juta jiwa, sementara diketahui pengguna perangkat Mobile mencapai 355.5 juta. Artinya peredaran ponsel pintar lebih banyak dari jumlah penduduk di seluruh Indonesia, hal ini dapat terjadi karena satu orang memiliki 2 atau lebih perangkat mobile (Websindo, 2019).



Gambar 1.2

Pengguna *Smartphone* di Indonesia

Sumber: websindo.com

Banyaknya jumlah pengguna *smartphone* yang ada di Indonesia, juga mendorong vendor *smartphone* untuk mengembangkan pembaharuan sistem operasi yang mereka miliki agar dapat melindungi data konsumennya. Seperti halnya yang dilakukan oleh perusahaan Apple, dimana mereka melakukan pembaharuan sistem operasi yang merupakan hal penting karena pelanggaran keamanan maupun privasi penggunanya menjadi suatu masalah yang serius. Apple sendiri sudah sejak lama dikenal ahli dalam hal keamanan untuk konsumennya karena perusahaan Apple sangat memprioritaskan privasi penggunanya, sehingga pengguna dapat merasa aman mengetahui data pribadi miliknya tidak disimpan atau dibaca oleh Apple maupun orang lain karena data pribadi pengguna sudah dienkripsi. Tidak dapat disangkal bahwa iOS adalah platform yang paling aman dan yang paling melindungi privasi pengguna. Jika pengguna peduli dengan privasi dan keamanan data pribadinya, maka Iphone adalah jawabannya (Fanatek, 2019).

Pada dasarnya Apple (iOS) sendiri merupakan OS (*Operating System*) yang diciptakan sendiri oleh perusahaan Apple Inc. Berbeda dengan *Mobile Operating System* lainya seperti Android yang dikembangkan oleh google dengan sifatnya *Open Source* dimana pengguna dapat secara bebas untuk melakukan pengubahan sesuai dengan keinginan dan selera yang biasa di sebut dengan AOSP, sebagai

contoh custom Rom. Sebaliknya pada *Mobile Operating System* iOS, penggua tidak dapat melakukan kebebasan seperti pada sistem operasi Android karena sifatnya yang *Close Source.* Sebenarnya, open source Android bisa menjadi keunggulan, namun bisa juga menjadi kelemahan, sebab keterbukaan pengembang ini nantinya bisa jadi akan dimanfaatkan oleh orang-orang yang tidak bertanggunga jawab, sehingga menyebabkan eror pada OS Android yang digunakan. Tentunya setiap OS baik Android maupun Apple (iOS) memiliki keunggulan masing-masing dari fitur kecanggian dan aplikasi yang dibawa, terdapat juga toko aplikasi resmi yang dimiliki oleh Apple yaitu *App Store* untuk mendownload berbagai macam aplikasi yang ingin digunakan (IDCloudhost, 2017).

Menurut Akraman *et al*., (2018), mengatakan bahwa informasi privasi menjadi salah satu kekhawatiran diantara pengguna platform *mobile* akan kehilangan privasi akibat pengungkapan informasi kepada pihak ketiga seperti developer aplikasi. Menurut Xu *et al*., (2012), mengatakan bahwa perkembangan Teknologi Informasi pada perangkat seluler dan *smartphone* telah memberikan pengalaman bagi pengguna *smartphone* dalam hal mengakses internet yang belum pernah dirasakan sebelumnya serta layanan nilai tambah yang didapat saat penggunaannya. Praktik agresif seperti pengaksesan data dan transmisi yang digunakan oleh aplikasi pada perangakat selular dan sistem operasi telah memperburuk masalah privasi pada pengguna *smartphone*. Berikutnya pada Tabel 1.1 dibawah ini telah disajikan beberapa contoh kasus pelanggran privasi yang terjadi pada pengguna OS iOS Apple.

Tabel 1.1

Daftar Kasus Pelanggaran Privasi Apple (iOS) Tahun 2015-2018

No	Tahun	Peristiwa	Sumber
1	22/10/2015	Analis keamanan telah menemukan setidaknya 256 aplikasi iOS di App Store yang diam-diam mengumpulkan alamat e-mail pemilik iPhone, nomor seri yang unik iPhone/iPad, dan informasi pribadi lainnya yang bisa digunakan untuk melacak pengguna. Apple App store memiliki proses pemeriksaan dan kebijakan privasi	Internetsehat.id (2015)

(Bersambung)

(Sambungan Tabel 1.1)

		yang sangat ketat terkait dengan pengumpulan data pribadi. Namun, pengumpulan data dilakukan secara sembunyi-sembunyi sehingga bahkan pengembang individu dari aplikasi yang terkena dampak tidak mungkin tahu tentang hal tersebut karena informasi pribadi yang dikirim hanya untuk pembuat kit pengembangan perangkat lunak yang digunakan untuk memberikan iklan dalam aplikasi tersebut. Menanggapi temuan ini Apple mengeluarkan pernyataan yang mengkonfirmasi keberadaan aplikasi yang secara diam-diam mengoleksi data pribadi pengguna sebagai bentuk pembayaran, yang kemudian mereka jual kepada pengiklan. Apple sudah mengidentifikasi sekelompok aplikasi yang menggunakan third-party advertising SDK yang dikembangkan oleh Youmi (China), penyedia iklan mobile, menggunakan private API untuk mengumpulkan informasi pribadi, seperti alamat email pengguna dan nomor pengenal perangkat, dan mengarahkan data ke server mereka. Apple mengatakan bahwa hal tersebut adalah pelanggaran pedoman keamanan dan privasi Apple.	
2	24/4/17	Pada tahun 2015, Uber dikatakan menemukan sebuah cara rahasia untuk mengidentifikasi dan melakukan tag (melacak lokasi) kepada pengguna iPhone yang memakai aplikasinya. Parahnya lagi, identifikasi tersebut konon tetap bisa dilakukan meski aplikasi Uber sudah dihapus oleh pengguna. Praktik identifikasi yang dikenal sebagai fingerprinting tersebut merupakan hal terlarang. Apple pun mengategorikan kegiatan itu sebagai pelanggaran privasi. Meski mengetahui larangan tersebut, Uber tetap nekat mempraktekan fingerprinting. Bahkan perusahaan	Hastyadi Widiartanto, Yoga (2017)

(Bersambung)

(Sambungan Tabel 1.1)

		ride sharing itu sengaja memasang geofence di markas Apple di Cupertino agar tidak ketahuan melakukan praktik terlarang. Geofence merupakan pagar virtual yang disematkan melalui GPS. Pagar ini bisa diatur agar mematikan aplikasi saat masuk ke wilayah tertentu dan menyalakannya lagi ketika pengguna aplikasi sudah berada di luar wilayah itu. Selain memasang geofence, Uber juga berani mengubah kode dalam aplikasi mereka agar tindakan fingerprinting itu tidak ketahuan pegawai Apple. Namun pada akhirnya hal tersebut diketahui pihak Apple segera melakukan tindakan menghentikan praktik fingerprinting tersebut.	
3	14/3/2018	Penipuan lewat email semakin luas dan kini menyerang pemilik iPhone dan Mac, meskipun Apple telah memperbarui tips yang dapat membantu pengguna melindungi diri dari penipuan phishing. Intinya, email tersebut merupakan pesan resmi dari Apple Store dengan informasi tentang langganan bulanan baru. Cybercriminals menetapkan tingkat berlangganan bulanan yang sangat tinggi untuk mencoba dan memaksa pengguna menekan tautan "Batalkan Langganan" di badan email. Mengeklik tautan tersebut akan mengarahkan pengguna ke laman web baru tempat peretas mencoba meminta kredensial masuk, ID kredit atau kartu debit Apple Anda, dan informasi pribadi lainnya. Namun, satu hal yang sangat perlu Anda ketahui, Apple tidak akan pernah meminta informasi pribadi melalui email, seperti kartu kredit atau kode CCV. Salah satu cara umum untuk melihat apakah sebuah email sah atau tidak adalah dengan mengecek alamat pengirimnya. Jika	Novianty (2018)

(Bersambung)

(Sambungan Tabel 1.1)

		email tidak berasal dari domain web Apple, kemungkinan itu bukan email yang asli.	
4	12/10/2018	Ant Financial (perusahan pemilik Alipay) dan Tencent Holdings memperingatkan adanya kejahatan cyber yang dilakukan hacker China. Mereka menyolong akun Apple ID untuk mencuri uang di layanan keduanya. Pun begitu, baik Alipay dan Tencent tidak menyebutkan berapa uang yang telah dicuri hacker. Namun keduanya memastikan telah menghubungi Apple untuk bekerjasama mengungkap masalah ini lebih detail. Baik Alipay maupun Tencent pun menghimbau para pengguna yang memiliki Apple ID yang terhubung dengan layanan pembayaran mereka untuk menurunkan batasan transaksi untuk mencegah kerugian yang besar pada pengguna. Selain itu, mereka juga merekomendasikan agar pengguna mengambil langkah-langkah preventif pada akun Apple-nya, misalnya mengubah password sesegera mungkin. Pasalnya, banyak pelanggan Alipay dan WePay sebagai pengguna iPhone, mereka menautkan dompet digital dengan Apple ID-nya. Setelah memperoleh akses, pencuri *online* dapat mentransfer uang tunai ke akun eksternal. Layanan pembayaran digital telah menjadi sasaran yang menggiurkan bagi pencuri cyber karena popularitas mereka meningkat di seluruh dunia.	Fida Rahman, Adi (2018)

Sumber: data yang telah diolah

Dari beberapa contoh kasus diatas dapat disimpulkan bahwa meskipun sistem operasi (iOS) ciptaan perusahaan Apple yang diclaim paling aman dan dapat melindungi data privasi penggunanya, ternyata data penggunanya masih dapat diambil tanpa sepengetahuan sebelumnya seperti yang dilakukan oleh Youmi pihak

ketiga sebagai developer aplikasi yang terdapat pada App Store, dimana pihak ketiga dalam App Store tersebut secara diam-diam mengumpulkan data pribadi milik pengguna *smartphone* Apple tersebut. Apple App store sendiri memiliki proses pemeriksaan dan kebijakan privasi yang sangat ketat terkait dengan pengumpulan data pribadi. Kemudian Apple mengeluarkan pernyataan yang mengkonfirmasi bahwa hal tersebut adalah pelanggaran pedoman keamanan dan privasi Apple. Selain itu, terdapat juga tindakan yang dilakukan secara sengaja oleh salah satu Aplikasi yaitu Uber yang secara terang terangan meskipun sudah diperingatkan oleh Apple terkait pelacakan lokasi pengguna *smartphone* Apple yang menggunakan jasa mereka, sehingga menyebabkan lokasi penggunanya dapat diketahui meskipun sudah menguninstall Applikasi uber tersebut. Masalah penipuan dan pencurian Apple ID juga dihadapi oleh pengguna *smartphone* Apple, dimana para pelaku meminta penggunanya Apple ID yang terhubung dengan layanan pembayaran untuk mengklik sebuah tautan yang akan diarahkan ke web peretas, sehingga peratas tersebut dapat mengambil informasi yang mereka butuhkan.

Beberapa contoh kasus diatas memiliki keterkaitan dengan variabel informasi privasi yang digunakan dalam pelitian ini, seperti pada contoh kasus pertama terdapat tindakan yang dilakukan oleh Youmi pihak ketiga sebagai developer aplikasi yang terdapat pada App Store, dimana pihak ketiga dalam App Store tersebut secara diam-diam mengumpulkan data pribadi milik pengguna *smartphone* Apple tersebut. Hal ini berkaitan dengan variabel *Secondary Use of Information* (penggunaan informasi untuk tujuan sekunder). Pada contoh kedua terdapat tindakan yang dilakukan oleh Uber yang dapat memantau penggunanya meskipun pengguna tersebut sudah menghapus applikasi Uber pada *smartphone*nya. Hal ini berkaitan dengan variabel *Perceived Surveillance* (aplikasi *mobile* dapat memantau kegiatan pengguna dan mengumpulkan banyak informasi), variabel *Perceived Intrusion* (rasa tidak nyaman pengguna akibat penggunaan informasi yang tidak sah) dan variabel *Secondary Use of Information* (penggunaan informasi untuk tujuan sekunder). Selanjutnya pada contoh ketiga terdapat tindakan penipuan yang mengarahkan pengguna untuk mengklik tautan berlangganan baru pada App Store

yang mengarahkan kepada situs peretas. Hal ini berkaitan dengan variabel *Disclosing Personal Information* (kekhawatiran pengungkapan informasi pribadi pengguna untuk mendapatkan manfaat tertentu) dan variabel *Secondary Use of Information* (penggunaan informasi untuk tujuan sekunder). Kemudian pada contoh kasus keempat terdapat tindakan pencurian yang dilakukan *Hacker* asal cina yang berusaha membobol Apple ID pengguna yang terhubung dengan layanan pembayaran. Hal ini berkaitan dengan variabel *Secondary Use of Information* (penggunaan informasi untuk tujuan sekunder).

Dari ringkasan contoh kasus tersebut menunjukan bahwa, data pribadi yang dimiliki oleh pengguna *smartphone* Apple rentan mengalami gangguan privasi yang disebabkan oleh kurangnya kesadaran pengguna *smartphone* Apple terhadap upaya untuk menjaga informasi pribadi miliknya saat menggunakan *smartphone* nya. Selain itu, sistem operasi (iOS) yang diclaim Apple paling aman ternyata belum sepenuhnya membuat konsumen pengguna *smartphone* Apple terhindar dari ancaman gangguan privasi.

Oleh karena itu, beberapa hal diatas yang menjadi landasan bagi penulis dalam melakukan penelitian mengenai kesadaran rivasi pada pengguna *smartphone,* lebih khususnya pengguna dari *smartphone* Apple dengan sistem operasi iOS yang akan diukur menggunakan dimensi *Attitude, Knowledge, Behavior* dengan fokus area *Perceived Surveillance, Perceived Intrusion, Secondary Use of Information,* dan *Disclosing Personal Information.*

1.3 Perumusan Masalah

Menurut Xu *et al*., (2012) mengungkapkan bahwa praktik agresif seperti pengaksesan data dan transmisi yang digunakan oleh aplikasi seluler dan sistem operasi telah memperburuk masalah privasi di antara pengguna. Kekhawatiran ini terkait dengan pengumpulan data secara otomatis, informasi komunikasi *real-time* pengguna, dan kerahasiaan data yang dikumpulkan seperti lokasi, identitas pribadi, dan perilaku sehari-hari. Praktik pengumpulan dan transmisi data yang agresif seperti itu menunjukan bahwa aliran informasi pada perangkat seluler bergerak ke domain kolektif di mana subjek data (misalnya, pengguna ponsel) dan penerima

data (misalnya, vendor atau penyedia aplikasi) menjadi pemilik bersama dengan tanggung jawab bersama untuk merahasiakan informasi tersebut. Karena alasan ini, kekhawatiran pengguna seluler untuk pengungkapan informasi pribadi milik mereka tidak dapat sepenuhnya dipahami, tanpa mengetahui harapan pengguna tentang bagaimana informasi yang diungkapkan akan digunakan dan siapa yang akan memiliki akses ke informasi tersebut. Hal yang diungkapkan oleh Xu *et al*., (2012) menunjukan bahwa sistem operasi (iOS) yang sudah diclaim memiliki keamanan yang baik masih beresiko terhadap ancaman gangguan privasi, dan dari contoh kasus yang dipaparkan di latar belakang menunjukan bahwa data pengguna dari *smartphone* Apple rentan terhadap ancaman gangguan privasi yang disebabkan rendahnya kesadaran penggunanya serta sistem operasi (iOS) yang diciptakan oleh Apple ternyata belum sepenuhnya membuat konsumen pengguna *smartphone* Apple terhindar dari ancaman gangguan privasi.

Beberapa hal tersebut yang melandasi penulis tertarik untuk melihat bagaimana kesadaran privasi (*Awareness Privacy*) pengguna *smartphone* Apple (iOS) dalam menggunakan media (*Smartphone*) khususya di Indonesia pada era Teknologi Informasi saat ini dengan penelitian yang berjudul **"PENGUKURAN KESADARAN PRIVASI PADA PENGGUNA *SMARTPHONE* APLLE (iOS) DI INDONESIA".**

1.4 Pertanyaan Penelitian

Berdasarkan latar belakang diatas, maka dapat diidentifikasikan masalah utama yang akan dipilih sebagai topik dari penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat *Privacy Awareness* pengguna *Smartphone* Apple (iOS) di Indonesia berdasarkan dimensi *Attitude*?
2. Bagaimana tingkat *Privacy Awareness* pengguna *Smartphone* Apple (iOS) di Indonesia berdasarkan dimensi *Knowledge*?
3. Bagaimana tingkat *Privacy Awareness* pengguna *Smartphone* Apple (iOS) di Indonesia berdasarkan dimensi *Behavior*?

1.5 Tujuan Penelitian

Berdasarkan latar belakang, perumusan masalah, dan pertanyaan penelitian yang telah diuraikan, maka tujuan dari penelitian ini sebagai berikut:

1. Untuk mengukur tingkat *Privacy Awareness* dari penggguna *Smartphone* Apple (iOS) di Indonesia berdasarkan dimensi *Attitude*?
2. Untuk mengukur tingkat *Privacy Awareness* dari penggguna *Smartphone* Apple (iOS) di Indonesia berdasarkan dimensi *Knowledge*?
3. Untuk mengukur tingkat *Privacy Awareness* dari penggguna *Smartphone* Apple (iOS) di Indonesia berdasarkan dimensi *Behavior*?

1.6 Manfaat Penelitian

Manfaat penelitian yang dapat diperoleh dari penelitian ini dibagi menjadi dua aspek yaitu:

1.6.1 Aspek Teoritis

Hasil penelitian ini diharapkan akan dapat melengkapi dunia keilmuan di bidang Sistem Informasi Manajemen yang terkait dengan *Security Management* khususnya mengenai masalah *Privacy Awareness,* dimana *Awareness* pengguna (manusia) yang menjadi salah satu komponen dalam ilmu Sistem Informasi Manajemen. Selian itu hasil temuan dalam penelitian ini serta dimensi yang digunakan seperti *Attitude, Knowledge, Behavior* (Kruger & Kearney, 2006) dan 4 fokus area yaitu *Perceived Surveillance, Perceived Intrusion, Secondary Use of Information* (Akraman *et al*., 2018) dan *Disclosing Personal Information* (Ginosar & Ariel, 2017) diharapkan dapat menjadi rujukan bagi penelitian berikutnya.

1.6.2 Aspek Praktis

Hasil dari penelitian mengenai pengukuran *Privacy Awareness* pada pengguna *smartphone* khususnya pada *smartphone* Apple (iOS) ini akan memiliki nilai yang baik dalam memberikan pengetahuan serta masukan bagi para pengguna *smartphone* Apple di Indonesia. Manfaat bagi pengguna *smartphone* Apple (iOS) dalam penelitian ini diharapkan dapat memberikan pemahaman kepada pengguna *smartphone* Apple (iOS) agar lebih waspada dalam menggunakan fitur-fitur yang ada didalam *smartphone* serta aplikasi yang terdapat pada *smartphone* mereka

dalam upaya melakukan penyebaran informasi didalamnya. Selain itu manfaat bagi pengguna *smartphone* Apple (iOS) dari segi *Awareness* lebih kepada memberikan rekomendasi dalam upaya menjaga data mereka seperti informasi pribadi dan informasi penting lainnya agar tidak disalahgunakan.

1.7 Ruang Lingkup Penelitian

1.7.1 Lokasi dan Objek Penelitian

Lokasi dan Objek yang digunakan oleh peneliti adalah sebagai berikut:

1. Penelitian ini dilaksanakan di Indonesia.
2. Objek dari penelitian ini adalah pengguna *Smartphone* Apple (iOS)

1.7.2 Waktu dan Periode Penelitian

Secara keseluruhan penelitian ini akan dilaksanakan dalam waktu 8 bulan terhitung sejak bulan September 2018 hingga Mei 2019. Penelitian ini terbagi dalam beberapa periode yaitu survei pendahuluan, usulan penelititan, kegiatan lapangan seperti pembagian kuesioner kepada responden, pengolahan dan analisis data, hingga penyelesaian penelitian.

1.7.3 Variabel Penelitian

Penelitian ini menggunakan 2 variabel, yaitu sebagai berikut:

1. *Awareness Level*, dengan sub variabel sebagai berikut:
   a. *Atttitude*
   b. *Knowledge*
   c. *Behavior*
2. *Information Privacy*, dengan sub variabel sebagai berikut:
   a. *Perceived Surveillance*
   b. *Perceived Intrusion*
   c. *Secondary Use of Information*
   d. *Disclosing Personal Information*

1.8 Sistematika Penulisan Tugas Akhir

Penulisan penelitian ini terdiri dari 5 bab yang bertujuan untuk memberikan gambaran apa yang terkandung dalam permasalahan yang dibahas sehingga didapatkan kesimpulan dari penelitian ini. Secara umum, peneliti menyusun sistematika penulisan penelitian sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan secara umum objek penelitian, latar belakang masalah, perumusan masalah, tujuan penelitian, kegunaan penelitian secara teoritis dan praktis, serta sistematika penulisan tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab ini menguraikan mengenai landasan teori yang digunakan sebagai dasar dari analisis penelitian khususnya mengenai audit. Bab ini memaparkan penelitian terdahulu sebagai acuan dasar dalam penelitian ini, pengembangan kerangka pemikiran, dan hipotesis penelitian sebagai jawaban sementara dalam penelitian ini.

BAB III METODE PENELITIAN

Bab ini menjelaskan mengenai karakteristik penelitian, metode dan teknik yang digunakan untuk pengumpulan, tahapan penelitian, populasi dan sampel, pengumpulan data, sumber data, serta teknik analisis dan pengujian hipotesis.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini membahas deskripsi hasil penelitian dan data yang diperoleh, sehingga diperoleh suatu kesimpulan yang digunakan dalam pengembangan teori penelitian selanjutnya.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran dari hasil penelitian yang dilakukan. Saran yang disajikan dapat digunakan pertimbangan dalam penelitian selanjutnya