SOURCE: Jurnal Ilmu Komunikasi
P-ISSN : 2477-5789
E-ISSN : 2502-0579

SOURCE: Jurnal Ilmu Komunikasi
Program Studi Ilmu Komunikasi
Universitas Teuku Umar
http://jurnal.utu.ac.id/jsource

PENGARUH KESADARAN KEAMANAN INFORMASI DAN PRIVASI JARINGAN SOSIAL TERHADAP PERILAKU PERLINDUNGAN PRIVASI PADA PARA PENGGUNA JARINGAN SOSIAL

Novita Chris[1], Tri Susanti[2], Nelson Donglas[3], Calvin Yantson[4], Vincent[5]

Program Studi Sistem Informasi - Universitas Internasional Batam

Abstract

Social networks are communication media that are used for sharing information and communicating. However, the popularity of social networks's user can not cover the anxiety about the privacy of user information data. This study aims to examine the factors that influence user anxiety about data security and security behavior. This study consists of five variables, namely response efficacy, self-efficacy, security awareness, and perceived security threat as an independent variable and internet user information privacy concern, and security behavior as the dependent variable. This study is a quantitative study that collects data and distributes questionnaires. The data in the study were analyzed through structural equation modeling (SEM) techniques with the help of SPSS. From the results of the study, this study proves that user perceptions of security threats (perceived security threats) have a significant effect on user anxiety about data privacy security when accessing social networks (Internet Users' Information Privacy Concern). This research provides insight to social network users to be more selective in managing data information security in providing personal data and taking protective actions against security behavior.

Keywords
Structural Equation Modelling (SEM)
Internet Users' Information Privacy Concern (IUIPC)
user awareness

Correspondence Contact
1931139.novita@uib.edu

PENDAHULUAN

Saat ini, jaringan sosial yang merupakan bagian dari media sosial telah menjadi pilihan utama sebagai media komunikasi yang sangat penting bagi masyarakat (Zlatolas et al., 2015). Indonesia mengalami kenaikan angka pada jumlah pengguna internet sebanyak 15.5% dari total pengguna pada tahun sebelumnya. Sebesar 84% dari total keseluruhan merupakan pengguna aktif media sosial dengan rata-rata menghabiskan waktu pada media sosial sekitar 3 jam 14 menit dalam sehari (Kemp, 2021). Populasi yang semakin muda membuat waktu penggunaan media sosial lebih tinggi, karena keterlibatan akan suatu hal yang lebih banyak dilakukan oleh para generasi muda. Penggunaan jaringan sosial sendiri memberikan manfaat yang bervariasi kepada penggunanya antara lain meningkatkan kenyamanan berkomunikasi dan berbagi informasi antar sesama (Chang et al., 2017).

Untuk dapat menggunakan layanan jaringan sosial, pengguna harus mengikuti langkah-langkah yang telah disediakan. Pada akses pertama, pengguna akan diarahkan untuk mengisi beberapa informasi pribadi yang diperlukan untuk proses pendataan internal. Informasi pribadi tersebut berupa komponen yang dinamis seperti lokasi, email dan juga karakteristik personal seperti latar belakang pribadi dan informasi kontak (Aghasian et al., 2017). Setelah memberikan data informasi, jaringan sosial akan memunculkan ketentuan yang memuat keamanan privasi untuk dapat dipahami oleh pengguna terlebih dahulu. Semenjak awal diluncurkan, ketentuan-ketentuan ini terus mengalami perkembangan. Sebagai contoh, Facebook dan WhatsApp kini sudah menggunakan pengendalian user centric berupa pengendalian privasi bagi para pengguna untuk mengatur sendiri siapa yang berhak mengakses informasi data yang diberikan. Ketentuan mengenai pengendalian akses

pengguna yang terus bertambah ternyata mempengaruhi pengguna untuk memberikan informasi data pribadi yang lebih banyak. Demi untuk mendapatkan dan menggunakan fitur yang baru, pengguna rela untuk memberikan informasi tambahan berupa informasi personal dan demographic (Soumelidou & Tsohou, 2019). Sebagai contoh, pengguna mengunggah foto dan video liburan pada akun jaringan sosial dengan mencantumkan lokasi dari tempat yang dikunjungi. Faktanya, informasi-informasi tersebut bisa saja diakses oleh orang luar dan dimanfaatkan secara tidak sadar dan tidak diketahui oleh pengguna.

Perkembangan ketentuan keamanan akses pengguna tidak selalu direspon positif oleh pengguna. Menurut penelitian, pembaruan ketentuan privasi WhatsApp pada tahun 2021 mendapatkan respon negatif dari perilaku penggunanya. Whatsapp telah mengizinkan platform jaringan sosial Facebook untuk mengelola informasi, menggunakan data, dan menambahkan pengumpulan data dari WhatsApp. Salah satu poin yang tertulis berbunyi data pengguna yang tercatat akan disimpan pada pusat data Facebook di seluruh dunia (Wijoyo et al., 2021). Hasil menunjukan bahwa semua yang diwawancarai mengetahui keberadaan ketentuan tersebut dan menyesalkan adanya ketentuan baru ini karena dianggap dapat membahayakan keamanan data pengguna seperti dokumen, pesan suara dan percakapan. Oleh sebab itu, pengguna mulai memikirkan untuk menggunakan platform media sosial lainnya.

Hingga tahun ini, banyak kasus yang melibatkan kebocoran informasi pribadi pengguna pada platform media sosial, termasuk kasus data pribadi Facebook yang diperjualbelikan ke perusahaan lain demi kepentingan pemetaan informasi calon konsumen (Iman et al., 2020). Hal ini yang kemudian menimbulkan Internet Users' Information Privacy Concern (IUIPC) (Zeng et al., 2020). IUIPC merujuk pada kecemasan yang dimiliki oleh pengguna internet terhadap cara suatu organisasi mengendalikan ketentuan yang dapat mempengaruhi keamanan dari informasi data privasi pengguna (Mohamed & Ahmad, 2012). Kekhawatiran tersebut juga berasal dari adanya tindakan membagikan informasi antara lain berupa pencurian identitas, cyber stalking atau e-stalking, blackmail dan juga personal spam (Nade, 2019).

Tujuan dari penelitian ini adalah untuk mencari validitas secara empiris dan kuantitatif dari variabel yang mempengaruhi IUIPC atau masalah privasi informasi pengguna dan menganalisis apakah IUIPC ini mempengaruhi tindakan melindungi privasi pada cakupan jaringan sosial (Adhikari & Panda, 2018). Penulis berharap penelitian ini dapat mempengaruhi perhitungan tingkat kesadaran keamanan privasi para pengguna dan membantu mengukur keamanan privasi dengan tingkat kesadaran yang diperlukan dalam penggunaan jaringan sosial (Aghasian et al., 2017).

KAJIAN TEORITIK

Penelitian ini didasarkan pada konseptual dan hasil penelitian sebelumnya. Salah satunya adalah penelitian mengenai pengaruh keamanan privasi terhadap perilaku keamanan yang dihasilkan pengguna. Penelitian ini menggunakan pendekatan security belief model yang menganalisa pengetahuan keamanan pengguna, kesadaran ancaman privasi, dan persepsi pengguna terhadap perilaku pengguna dalam menggunakan media sosial Line. Analisa pada penelitian ini dilakukan dengan hasil kuesioner dari 263 data responden pengguna Line dengan pendekatan tipe model Structural Equation Modeling (SEM). Hasil yang didapatkan adalah kesadaran terhadap kesadaran ancaman privasi dan pengetahuan keamanan pengguna memiliki pengaruh yang signifikan terhadap persepsi pengguna dalam menentukan perilaku dalam menggunakan media sosial Line (Afandi et al., 2017).

Penelitian selanjutnya adalah penelitian mengenai kontekstualisasi bagaimana remaja mengelola privasi pribadi dan interpersonal mereka dalam menggunakan sosial media. Penelitian ini mempelajari manajemen privasi para remaja di sosial media dan bagaimana

tindakan mereka dalam mengawasi dan mengatur informasi secara individual. Analisa penelitian ini lebih mengutamakan remaja sebagai target utama dan menggunakan pendekatan kerangka teoritis Communication Privacy Management (CPM). Penelitian ini membuktikan bahwa perasaan fatalisme yang dialami remaja mengenai pengendalian diri dalam lingkungan social networking atau dikenal dengan networked defeatism berhubungan positif dengan manajemen privasi interpersonal dimana manajemen privasi ini kurang diperhatikan saat berkomunikasi mengenai batasan pribadi (personal boundaries) bersama rekan kerja dibandingkan pada saat berkomunikasi mengenai pembahasan seksual dan menangani informasi pribadi yang dibagikan oleh orang tua (Wolf, 2020).

Penelitian berikutnya adalah penelitian mengenai pengaruh kecemasan pengguna internet terhadap perilaku keamanan oleh pengguna media sosial. Penelitian ini menggunakan pendekatan dengan mendeskripsikan pengetahuan ancaman privasi dan juga kepercayaan potensi diri dalam menjaga keamanan yang dapat mempengaruhi kecemasan pengguna terhadap privasi mereka di media sosial. Penelitian ini melakukan uji terhadap 306 data responden kuesioner yang digunakan pada analisa tahap akhir dengan pendekatan tipe model Structural Equation Modeling (SEM). Hasil dari penelitian ini membuktikan bahwa kepercayaan ancaman privasi dan akibat yang dihasilkannya memiliki pengaruh yang signifikan terhadap kecemasan privasi pengguna. Namun, faktor lain berupa manfaat lebih media sosial dan kepercayaan terhadap potensi diri dalam menjaga keamanan tidak berpengaruh terhadap kecemasan privasi pengguna dalam menggunakan internet (Adhikari & Panda, 2018).

Penelitian selanjutnya adalah penelitian mengenai hubungan antara kesadaran privasi, keamanan privasi dan kecemasan pribadi. Penelitian ini berfokus pada keterbukaan seseorang dalam berbagi data yang dapat berdampak pada privasi para pengguna jaringan sosial Facebook. Analisa dalam penelitian ini dilakukan dengan mengumpulkan 661 responden yang berpartisipasi dalam survei online dengan pendekatan tipe model Structural Equation Modeling (SEM). Hasil yang didapatkan adalah kecemasan privasi dipengaruhi oleh keterbukaan seseorang dan kesadaran privasi mempengaruhi keterbukaan seseorang dalam berbagi informasi pada jaringan sosial Facebook (Zlatolas et al., 2015).

Penelitian selanjutnya adalah penelitian mengenai pengaruh dari visualisasi ketentuan privasi terhadap tingkat kesadaran keamanan informasi pengguna media sosial Instagram. Penelitian ini berfokus pada studi untuk menemukan teknik pemaparan ketentuan media sosial yang efektif yang dapat mempengaruhi peningkatan kesadaran keamanan pengguna. Penelitian ini menganalisis data dengan mengandalkan kasus ketentuan privasi pada instagram dan membuat 2 investigasi secara empirik. Melalui kuesioner yang telah diuji, peneliti kemudian menganalisa efek dari tiap teknik yang digunakan. Hasil dari penelitian ini adalah ketentuan keamanan menggunakan teknik visualisasi memberikan efek signifikan kepada kesadaran keamanan pengguna dibandingkan dengan ketentuan teks biasa (Soumelidou & Tsohou, 2019).

Penelitian berikutnya adalah penelitian mengenai tingkat kesadaran keamanan dari pengguna media sosial. Penelitian berfokus pada studi terhadap perkembangan ketentuan media sosial yang berkembang pada Indonesia. Dengan target penelitian berupa mahasiswa dari Universitas Indonesia, penelitian ini menggunakan pendekatan kualitatif untuk mengukur pengaruh tingkat kesadaran keamanan privasi pengguna terhadap personal data yang dibagikan pada media sosial. Penelitian ini membuktikan bahwa kesadaran pengguna akan muncul pada detik pengguna membagikan informasi pribadi tersebut pada media sosial (Iman et al., 2020).

Dasar penelitian selanjutnya adalah penelitian oleh mengenai pengaruh keamanan privasi terhadap kecemasan pengguna internet dalam menggunakan jaringan sosial. Penelitian ini mendeskripsikan kecemasan privasi dalam perspektif pengguna jaringan sosial dengan model IUIPC. Hal tersebut kemudian digunakan untuk menganalisis pengaruh informasi pribadi yang sensitif terhadap tindakan pengguna dalam memberikan informasi pribadi tersebut di cakupan jaringan sosial. Penelitian ini dilakukan dengan 168 data responden yang disebarkan dan diteliti dengan pendekatan tipe model Structural Equation Modeling (SEM). Penelitian ini memberikan kesimpulan bahwa informasi pribadi yang sensitif mengurangi tindakan pengguna dalam memberikan informasi pribadi di jaringan sosial. Selain itu, penelitian ini juga membuktikan IUIPC memiliki pengaruh yang signifikan terhadap kepercayaan ancaman privasi dan tidak signifikan terhadap kepercayaan keamanan privasi (Zeng et al., 2020).

Penelitian selanjutnya menerapkan model IUIPC yang digunakan untuk menyelidiki permasalahan privasi informasi terhadap penggunaannya di media sosial (Afandi et al., 2017). Penelitian mengenai privasi informasi personal pertama kali dikemukakan oleh Smith, Milberg & Burke (1996) dengan model Global Information Privacy Concern (GIPC) yang masih menjelaskan secara umum. Selanjutnya dikembangkan oleh Stewart & Seagaras (2002) menjadi model Concern for Information Privacy (CFIP) yang memformulasikan dimensi pembentuk atas privasi informasi personal dengan collection, error, unauthorized secondary used, dan improper access. Kemudian terjadi pertentangan terhadap model CFIP oleh Malhotra, Kim & Agarwal (2004) dengan mengemukakan model Internet Users' Information Privacy Concern (IUIPC) yang memformulasikan dimensi terkait awareness of privacy practices (Kusyanti et al., 2017).

Berdasarkan studi diatas, terdapat perbedaan dalam penggunaan cakupan media komunikasi yang digunakan untuk melakukan penelitian. Secara umum, beberapa penelitian menggunakan media komunikasi "media sosial" sebagai pedoman penelitian. Namun, penelitian yang menggunakan media komunikasi "jaringan sosial" hanya ditunjukan pada 1 studi. Penelitian kami akan dilakukan berdasarkan studi tersebut. Kami juga akan melakukan penelitian terhadap faktor yang mempengaruhi tindakan melindungi privasi ketika menggunakan layanan jaringan sosial yang didasarkan oleh penelitian (Soumelidou & Tsohou, 2019), (Wolf, 2020) dan (Iman et al., 2020). Kami juga akan meneliti komponen yang mempengaruhi IUIPC dan perilaku keamanan pengguna yang didasarkan oleh penelitian (Afandi et al., 2017) dan (Adhikari & Panda, 2018). Penelitian akan dilakukan dengan pendekatan kuantitatif seperti (Afandi et al., 2017), (Adhikari & Panda, 2018), (Zlatolas et al., 2015) dan (Zeng et al., 2020). Sampel yang akan digunakan dalam penelitian kami berasal dari pengguna jaringan sosial seperti (Zeng et al., 2020). Kontribusi dari penelitian kami adalah penelitian ini akan berfokus pada masyarakat Batam yang menggunakan jaringan sosial. Kami berharap penelitian ini dapat memberikan tambahan wawasan mengenai keamanan privasi di media sosial khususnya pada jaringan sosial.

METODOLOGI

Sampel dan Populasi, Teknik Pengumpulan Data dan Teknik Analisis Data

Metode yang digunakan dalam penelitian ini adalah metode kuantitatif. Populasi pada penelitian ini adalah masyarakat Batam, khususnya mahasiswa, pekerja, orang tua, dan pengajar pendidikan yang pernah dan sedang menggunakan jaringan sosial dengan menggunakan Stratified Disproportionate Random Sampling Method. Model penelitian yang digunakan adalah model Internet Users' Information Privacy Concern (IUIPC). Metode pengumpulan data dilakukan dengan membagikan kuesioner menggunakan Google Form yang disebarluaskan melalui media sosial seperti Instagram, Line, dan WhatsApp kepada

populasi dengan target sebanyak 385 sampel berdasarkan kalkulasi Raosoft terhadap jumlah masyarakat Batam. Data sampel yang terkumpul kemudian dilakukan pembagian berdasarkan durasi yang dihabiskan oleh pengguna ketika menggunakan jaringan sosial, yaitu dibawah 60 menit, 60-90 menit, dan penggunaan lebih dari 90 menit.

Metode analisis data yang kami gunakan yaitu pengujian kualitas data dengan melakukan uji validitas dan uji reabilitas dengan menggunakan program SPSS. Teknik pengujian validitas dilakukan dengan menggunakan korelasi Produk Momen Pearson (Bivariate Pearson) dengan koefisien korelasi yang signifikan akan dikatakan valid, sedangkan teknik pengujian reliabilitas dilakukan dengan menggunakan Cronbach alpha dengan standar lebih dari 0.6. Metode analisis hipotesis yang akan kami gunakan adalah metode SEM (Structural Equation Modeling) yang digunakan untuk menampilkan korelasi tiap variabel yang akan diuji. Pada tahap ini dilakukan analisis hipotesis dimana model yang telah memenuhi standar pengujian akan dibandingkan nilai antar variabel yang kemudian dianalisis dengan hipotesis (Zulaikhah et al., 2020).

Model dan Variabel Penelitian

Penelitian ini menerapkan model IUIPC yang digunakan untuk menyelidiki permasalahan privasi informasi terhadap penggunaannya di media sosial (Afandi et al., 2017). Kami menggunakan model modifikasi dari model IUIPC yang dikemukakan oleh Malhotra, Kim & Agarwal (2004). Secara spesifik, variabel independen dan dependen yang digunakan pada penelitian ini terdiri dari Response Efficacy, Self-efficacy, Security Awareness, dan Perceive Security Threat sebagai variabel independen dan Internet User Information Privacy Concern, dan Security Behavior sebagai variabel dependen.

Response Efficacy (RE)

Response Efficacy mengandung pengertian kepercayaan dalam perilaku keamanan yang telah disediakan melalui pengendalian dan perlindungan privasi dapat melindungi data pengguna dari berbagai ancaman yang ada di ruang lingkup internet (Mohamed & Ahmad, 2012).

Self-efficacy (SE)

Self-Efficacy dapat diartikan menjadi kepercayaan seseorang mengenai pengetahuan yang dimiliki untuk dapat melindungi data privasi mereka dari oknum yang tidak diketahui dan mengetahui perilaku keamanan yang dapat meminimalisir kebocoran informasi pada penggunaan jaringan sosial (Afandi et al., 2017).

Security Awareness (SA)

Security Awareness merupakan kemampuan yang dimiliki oleh seseorang dalam menerapkan perilaku keamanan ketika menggunakan jaringan sosial dan dapat memahami pentingnya perlindungan data privasi dalam menggunakan situs jaringan sosial (Afandi et al., 2017).

Perceive Security Threat (PST)

Perceive Security Threat mengandung pengertian kepercayaan seseorang terhadap adanya ancaman yang dapat membahayakan keamanan dari data personal informasi pengguna. Ancaman tersebut dapat berupa tindakan-tindakan mencuri dan membagikan informasi di internet (Adhikari & Panda, 2018).

Internet User Information Privacy Concern (IUIPC)

IUIPC merujuk pada kecemasan yang dimiliki oleh pengguna internet terhadap cara suatu organisasi mengendalikan ketentuan yang dapat mempengaruhi keamanan dari informasi data privasi pengguna (Mohamed & Ahmad, 2012). Kekhawatiran tersebut juga berasal dari adanya tindakan membagikan informasi antara lain berupa pencurian identitas, cyber stalking atau e-stalking, blackmail dan juga personal spam (Nade, 2019).

Security Behavior (SB)

Security Behavior mengandung pengertian perilaku atau tindakan seseorang dalam menghadapi dan melindungi informasi data privasi pengguna ketika menggunakan jaringan sosial. Security behavior juga merujuk kepada tingkat ketersediaan pengguna dalam membagikan data mereka di internet (Adhikari & Panda, 2018).

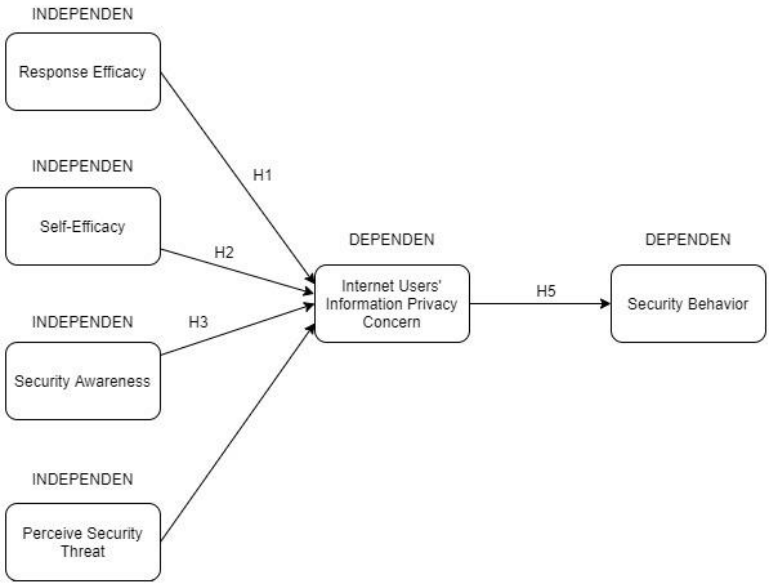

Fig. 3.1. Model Penelitian

Rumusan Hipotesis

Berdasarkan definisi variabel dan model penelitian sebelumnya, terdapat 10 rumusan hipotesis yang akan digunakan dalam penelitian ini:

1. H1A Tindakan dalam mencegah threat (response efficacy) mempengaruhi kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC)

2. H1o Tindakan dalam mencegah threat (response efficacy) tidak mempengaruhi mempengaruhi kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC)

3. H2A Kepercayaan pengguna mengenai pengetahuan yang dimiliki untuk dapat melindungi data pribadi (self-efficacy) (SE) mempengaruhi skala kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC).

4. H2o Kepercayaan pengguna mengenai pengetahuan yang dimiliki untuk dapat melindungi data pribadi (self-efficacy) (SE) tidak mempengaruhi kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC).

5. H3A Kemampuan yang dimiliki oleh pengguna dalam memahami dan menerapkan perilaku keamanan (security awareness) (SA) mempengaruhi kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC).

6. H3o Kemampuan yang dimiliki oleh pengguna dalam memahami dan menerapkan perilaku keamanan (security awareness) (SA) tidak mempengaruhi kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC).

7. H4A Kepercayaan seseorang terhadap adanya ancaman yang dapat membahayakan keamanan privasi (perceived security threat) (PST) mempengaruhi kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC).

8. H4o Kepercayaan seseorang terhadap adanya ancaman yang dapat membahayakan keamanan privasi (perceived security threat) (PST) dan kewajaran pengguna tidak mempengaruhi kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC).

9. H5A Kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC) mempengaruhi perilaku atau tindakan pengguna dalam menghadapi dan melindungi informasi data privasi (security behavior) (SB).

10. H5o Kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC) tidak mempengaruhi perilaku atau tindakan pengguna dalam menghadapi dan melindungi informasi data privasi (security behavior) (SB).

Definisi Operasional Variabel

Berdasarkan model penelitian yang telah dijelaskan sebelumnya, definisi operasional variabel yang digunakan dalam penelitian ini disajikan pada Tabel 1.

Table 1. Definisi Operasional Variabel

Definition Operational Variable			
Variable	Dimension	Indicator	References
Respon Efficacy (x1)	Control	RE1 Jika saya menggunakan pelindung keamanan (seperti anti-virus) di situs jaringan sosial, mungkin ini akan melindungi saya dari kehilangan informasi	(Mohamed & Ahmad, 2012)
		RE2 Saya bisa melindungi privasi informasi saya lebih baik lagi jika menggunakan pelindung keamanan di situs jaringan sosial	
		RE3 Menggunakan pelindung keamanan di situs jaringan sosial memastikan keamanan informasi saya tetap terjaga	
		RE4 Jika saya menggunakan pelindung keamanan, kecil kemungkinan informasi saya akan hilang	
Self-Efficacy in Information Security (X2)	Security Policy	SE1 Saya mengetahui bagaimana mengatur pengaturan privasi sehingga hanya kelompok tertentu yang bisa menerima informasi yang saya bagikan	(Soumelidou & Tsohou, 2019)
		SE2 Saya mengetahui secara persis siapa yang bisa melihat informasi yang saya bagikan di jaringan sosial	

Definition Operational Variable			
Variable	Dimension	Indicator	References
		SE3 Saya bisa mengaktifkan fitur perlindungan privasi di jaringan sosial tanpa bantuan orang lain	
		SE4 Saya yakin (dan percaya) saat menggunakan fitur perlindungan privasi di jaringan sosial	
Security Awareness (X3)	Awareness	SA1 Saya menyadari permasalahan privasi dan keamanan serta menerapkannya di jaringan sosial	(Zlatolas et al., 2015)
		SA2 Saya mengikuti perkembangan berita mengenai permasalahan privasi dan keamanan serta pelanggaran privasi	
		SA3 Saya terus memperbarui diri mengenai informasi permasalahan privasi dan keamanan serta solusi yang telah disediakan oleh pihak jaringan sosial untuk memastikan keamanan privasi saya	
		SA4 Saya mengetahui bagaimana melindungi diri dari penyalahgunaan data di jaringan sosial	
Perceived Security Threat (X4)	Risk beliefs	PST1 Saya merasa akan mengalami masalah keamanan online (seperti gangguan privasi, serangan virus, dll) di jaringan sosial	(Adhikari & Panda, 2018)
		PST2 Saya merasa informasi saya di jaringan sosial dapat disalahgunakan.	
		PST3 Saya merasa informasi saya di jaringan sosial dapat digunakan oleh pihak yang tidak dikenal tanpa sepengetahuan saya	
		PST4 Saya merasa informasi saya di jaringan sosial dapat digunakan oleh agensi pemerintah	
Internet Users' Information Privacy Concerns (Y1)	Collection	IUIPC1 Saya khawatir ketika mengirimkan informasi di jaringan sosial karena dapat digunakan untuk tujuan yang salah	(Adhikari & Panda, 2018)
		IUIPC2 Saya khawatir ketika mengirimkan informasi di jaringan sosial karena dapat diakses oleh pihak yang tidak dikenal	
		IUIPC3 Saya biasanya berpikir dua kali sebelum memberikan informasi di jaringan sosial	
		IUIPC4 Saya merasa jaringan sosial mengumpulkan informasi yang berlebihan	
		IUIPC5 Saya khawatir ketika memberikan informasi di jaringan sosial karena dapat digunakan ketika saya tidak menyadarinya	
Security Behavior (Y2)	Private Disclosure	SB1 Saya sering menghapus cookies dari browser saya	(Soumelidou & Tsohou, 2019)
		SB2 Saya dengan sadar memberikan informasi pribadi yang salah di jaringan sosial	(Adhikari & Panda, 2018)
		SB3 Saya dengan sadar memberikan informasi pribadi yang tidak lengkap di jaringan sosial	
		SB4 Saya dengan sadar memberikan informasi pribadi palsu di jaringan sosial	
		SB5 Saya dengan sadar menahan diri dalam memberikan informasi pribadi yang spesifik di jaringan sosial	

Definition Operational Variable			
Variable	Dimension	Indicator	References
		SB6 Saya dengan sadar menghindari pemberian informasi pribadi yang spesifik di jaringan sosial	
		SB7 Saya dengan sadar menolak untuk memberikan informasi pribadi yang spesifik di jaringan sosial	

HASIL DAN PEMBAHASAN

Analisa Data

A. Analisa Deskriptif

Berdasarkan jumlah data yang telah terkumpul dari penyebaran kuesioner melalui Google Form, terdapat sebanyak 434 data dengan sebanyak 38 data merupakan data outlier sehingga deskriptif responden untuk data sebanyak 396 dapat dilihat pada Tabel 2.

Table 2. Deskriptif Responden

Karakteristik Demografis	Frekuensi (% dari total)
Status responden	
Pelajar	354 (89,4%)
Pengajar	5 (1,3%)
Orang Tua	9 (2,3%)
Pekerja	28 (7,1%)
Usia	
<18	87 (22%)
18 - 24	296 (74,7%)
24 - 40	12 (3%)
> 40	1 (0.3%)
Durasi Mengakses Jaringan Sosial	
< 60 menit	136 (34,3%)
60 - 90 menit	135 (34,1%)
> 90 menit	125 (31,6%)

B. Uji Outlier Data

Data outlier adalah kasus data yang memiliki nilai yang unik dan sangat berbeda dengan data-data lainnya. Data outlier dimunculkan dengan nilai yang ekstrim. Penelitian ini menguji outlier dengan menggunakan analisis regresi linear. Pengukuran outlier diukur dengan melihat nilai studentized residual. Dari jumlah 434 data responden yang telah terkumpul, terdapat 38 data yang dinyatakan sebagai data outlier univariat, atau data dengan nilai data studentized residual lebih dari 3.

C. Uji Validitas dan Reliabilitas

Uji validitas adalah uji yang digunakan untuk menunjukkan sejauh mana alat ukur atau instrumen yang digunakan mampu mencapai tujuan penelitian yang diinginkan dan memberikan hasil yang tepat dan akurat. Sedangkan uji reliabilitas adalah uji yang digunakan untuk mengetahui kekonsistenan data dalam mengukur sasaran yang diukur. Nilai reliabilitas yang memenuhi standar reliabilitas atau lebih dari 0,06 menyatakan bahwa data yang terkumpul dapat memberikan ketepatan yang tinggi dan dapat untuk diandalkan. Uji validitas dilakukan dengan menggunakan korelasi bivariate pearson. Melalui korelasi bivariate pearson, penelitian ini melakukan penarikan kesimpulan berdasarkan nilai signifikansi Sig. (2-tailed) dan tanda bintang (*) yang diberikan oleh SPSS. Sedangkan untuk mengetahui reliabilitas dari suatu variabel, penelitian ini menggunakan nilai Cronbach Alpha dari variabel sebagai acuan dalam melakukan uji ini. Nilai Cronbach Alpha variabel yang dinyatakan memenuhi standar adalah harus lebih dari 0,06.

Berdasarkan pengujian validitas data yang telah dilakukan, analisis menunjukan bahwa semua instrumen variabel memiliki nilai signifikansi Sig. (2-tailed) kurang dari 0,05. Hal ini mengandung pengertian bahwa terdapat korelasi antar variabel. Selain itu, hasil uji juga memperlihatkan adanya tanda bintang pada nilai pearson correlation yaitu tanda bintang dua (**) pada semua instrumen variabel. Hal ini menunjukan bahwa korelasi yang terjadi memiliki signifikan sebesar 1% atau 0,01. Dengan kedua acuan tersebut, dapat dinyatakan bahwa semua instrumen variabel pada penelitian ini dinyatakan valid. Sedangkan untuk uji reliabilitas yang telah dilakukan, analisis menunjukan bahwa semua variabel memiliki nilai Cronbach Alpha lebih dari 0,06. Melalui acuan dari standar nilai Cronbach Alpha yang memenuhi syarat reliabilitas, dapat dinyatakan bahwa semua semua variabel pada penelitian ini dinyatakan dapat digunakan untuk mengukur kebenaran atau reliabel. Dengan hasil dari kedua uji validitas dan reliabilitas data diatas, dapat ditarik kesimpulan bahwa keenam variabel yang terdiri dari 4 variabel independen dan 2 variabel independen pada penelitian ini dinyatakan valid dan reliabel.

D. Uji Structural Model dan Hipotesis

Hipotesis dinyatakan diterima apabila pengujian nilai critical ratio (CR) lebih dari 1,96 dan p-value kurang dari 0,05. Hasil uji structural model dan hipotesis dapat dilihat dalam Tabel 3.

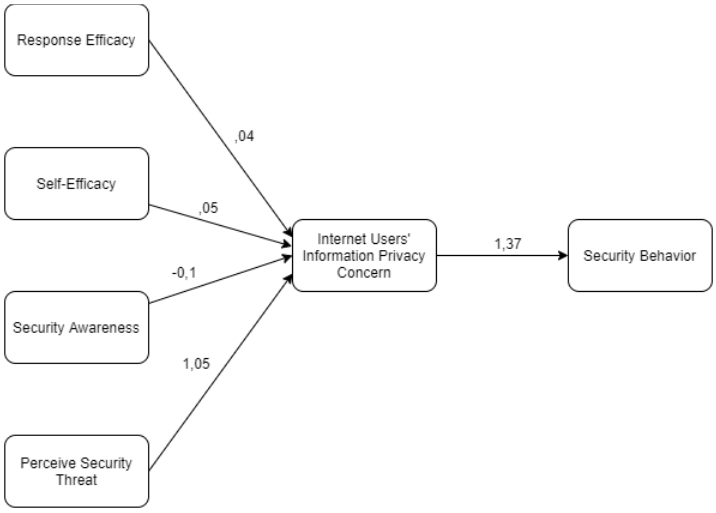

Fig. 4.1. Model Penelitian

Table 3. Hasil Uji Structural Model dan Hipotesis

Index	Estimate	S.E.	C.R.	P-Value
IUIPC ← SA	-,014	,036	-,392	,695
IUIPC ← RE	,038	,023	1,631	,103
IUIPC ← SE	,049	,037	1,321	,187
IUIPC ← PST	1,055	,100	10,568	***
SB ← IUIPC	1,371	,097	14,098	***

Pembahasan Hipotesis

Berdasarkan tabel 3 dapat disimpulkan melalui nilai critical ratio dan p-value bahwa terdapat 3 hipotesis penelitian yang dinyatakan diterima, dan 2 hipotesis penelitian yang dinyatakan tidak diterima.

Pembahasan Hipotesis H1

Berdasarkan hasil uji variabel yang telah dilakukan, hipotesis yang menyatakan ada hubungan antara kepercayaan seseorang terhadap perilaku keamanan yang ada (response efficacy) (RE) dan kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC) memberikan hasil hipotesis nol atau dinyatakan tidak mempengaruhi. Hal ini dikarenakan p-value yang dihasilkan dari hipotesis ini adalah sebesar 0,103 atau melebihi nilai batas p-value yang valid yaitu 0,05.

Pembahasan Hipotesis H2

Berdasarkan hasil uji variabel yang telah dilakukan, hipotesis yang menyatakan ada hubungan antara pengguna dalam memahami praktik keamanan informasi (self-efficacy) (SE) dan kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC) dinyatakan tidak signifikan atau ditolak. Hal ini dikarenakan p-value yang dihasilkan dari hipotesis ini adalah sebesar 0,187 atau melebihi nilai batas p-value yang valid yaitu 0,05. Hal ini mengandung pengertian bahwa kepercayaan seseorang mengenai pengetahuan yang dimiliki untuk dapat melindungi data privasi mereka dan mengetahui perilaku keamanan yang dapat meminimalisir kebocoran data ternyata tidak memberikan dampak signifikan pada tingkat kecemasan pengguna terhadap keamanan data privasi yang dimiliki.

Pembahasan Hipotesis H3

Berdasarkan hasil uji variabel yang telah dilakukan, hipotesis yang menyatakan kesadaran terhadap keamanan (security awareness) (SA) dan tingkat perhatian pengguna media sosial mempengaruhi kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC) dinyatakan tidak memiliki hubungan dan tidak saling mempengaruhi. Hal ini dikarenakan nilai estimate yang dihasilkan sebesar -0,014, critical ratio sebesar -0,392, dan p-value sebesar 0,695 yang telah melebihi batas nilai p-value itu sendiri yaitu 0,05. Hal ini mengandung pengertian bahwa kemampuan yang dimiliki seseorang dalam menerapkan perilaku perlindungan data privasi tidak mempengaruhi kecemasan pengguna dalam menggunakan internet.

Pembahasan Hipotesis H4

Berdasarkan hasil uji variabel yang telah dilakukan, hipotesis yang menyatakan persepsi pengguna terhadap ancaman keamanan (perceived security threat) (PST) dan kewajaran pengguna mempengaruhi kecemasan yang dimiliki oleh pengguna internet terhadap

keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC) dinyatakan memiliki hubungan positif yang signifikan. Hal ini dibuktikan dengan nilai estimate sebesar 1,055, critical ratio sebesar 10,568, dan nilai p-value ≤ 0,001. Hal ini mengandung pengertian bahwa pengguna merasa terdapat sebuah resiko atau ancaman pada informasi data privasinya ketika menggunakan internet dan akan melakukan tindakan preventif untuk menjaga informasi data privasinya agar tidak disalahgunakan.

Pembahasan Hipotesis H5

Berdasarkan hasil uji variabel yang telah dilakukan, hipotesis yang menyatakan kecemasan yang dimiliki oleh pengguna internet terhadap keamanan informasi dan data privasi (internet users' information privacy concerns) (IUIPC) mempengaruhi perilaku keamanan pengguna (security behavior) (SB) dinyatakan terdapat hubungan positif yang signifikan. Hal ini dibuktikan dengan nilai estimate sebesar 1,371, critical ratio sebesar 14,098, dan nilai p-value ≤ 0,001. Hal ini mengandung pengertian bahwa pengguna akan melakukan perilaku keamanan ketika menggunakan internet untuk melindungi informasi data privasinya ketika mereka memiliki kecemasan terhadap keamanan informasi data privasinya.

Pada bagian hasil dan pembahasan peneliti harus menjelaskan temuan dari penelitian yang dilakukan dan analisis secara mendalam sesuai dengan penekanan teori atau konsep yang digunakan. Pembahasan harus dituliskan secara jelas dan focus memberikan jawaban terhadap permasalahan yang dituju di pendahuluan. Peneliti dapat memaparkan temuan dan analisis dalam bentuk deskripsi, table, gambar, atau data. Bagi penelitian lapangan peneliti diharuskan juga menyebutkan kutipan hasil wawancara.

KESIMPULAN DAN IMPLIKASI

Kesimpulan

Berdasarkan hasil analisa data, dapat disimpulkan bahwa kepercayaan pengguna terhadap adanya ancaman yang dapat membahayakan keamanan dari data personal informasi (perceive security threat) dapat mempengaruhi rasa kecemasan pengguna dalam keamanan data tersebut (internet users' information privacy concerns). Penelitian ini sejalan dengan penelitian (Afandi et al., 2017). Ancaman-ancaman dalam konteks ini dapat berupa tindakan-tindakan mencuri dan membagikan informasi di internet (Adhikari & Panda, 2018). Penelitian membuktikan bahwa pengguna mempercayai bahwa ketika menggunakan jaringan sosial, pengguna dapat mengalami masalah keamanan data secara online dan data tersebut dapat disalahgunakan oleh pihak yang dikenal maupun agensi pemerintah. Setelah pengguna memahami adanya ancaman keamanan data tersebut, maka pengguna akan menjadi berhati-hati dalam mengakses jaringan sosial. Dengan kata lain, kecemasan terhadap keamanan data privasi ini menimbulkan urgensi pengguna untuk menerapkan perilaku keamanan (security behavior). Perilaku keamanan yang dilakukan pengguna dapat berupa ketidaksediaan pengguna dalam membagikan data mereka di internet secara sebagian ataupun penuh (Adhikari & Panda, 2018). Pengguna juga cenderung untuk menahan dan menghindari diri dalam memberikan data pribadi yang spesifik pada jaringan sosial.

Penelitian ini juga mengungkapkan faktor-faktor yang memiliki kontribusi sebaliknya. Kepercayaan seseorang terhadap perilaku keamanan yang ada (response efficacy), pengguna dalam memahami praktik keamanan informasi (self-efficacy), dan kesadaran terhadap keamanan (security awareness) tidak memberikan kontribusi terhadap kecemasan pengguna dalam keamanan data (internet users' information privacy concerns). Perilaku keamanan yang disediakan oleh jaringan sosial dapat berupa ketentuan keamanan akses pengguna yang telah dikembangkan pada hampir semua jaringan sosial agar pengguna dapat mengatur sendiri siapa yang berhak untuk mengakses data privasi yang dibagikan pengguna. Namun ternyata upaya platform jaringan sosial dalam mengembangkan ketentuan akses

pengguna tidak mempengaruhi tingkat kecemasan pengguna terhadap keamanan data privasi yang dimiliki. Hasil ini sejalan dengan penelitian (Adhikari & Panda, 2018). Penjelasan yang mengartikan kondisi ini dapat dikaitkan dengan mempertimbangkan pengalaman pengguna yang membentuk pemikiran dan kelakukan pengguna (Adhikari & Panda, 2018). Pengguna memiliki pengalaman nyata yang sedikit terhadap ancaman keamanan data, sehingga pengguna tidak menjadikan perilaku keamanan yang telah disediakan sebagai salah satu faktor yang penting ketika mengakses jaringan sosial.

Pengguna yang memiliki kepercayaan dalam memiliki keahlian dalam melindungi diri mereka terhadap ancaman privasi ternyata tidak memiliki dampak terhadap kecemasan pengguna. Melalui situasi ini, dapat diartikan menjadi ketika seseorang merasa dapat melindungi privasi mereka maka mereka hanya merasa telah memiliki pengetahuan yang lebih dan tidak dihubungkan dengan kecemasan. Kecemasan pengguna akan tetap ada pada semua pengguna yang mengakses jaringan sosial.

Kesadaran terhadap keamanan merujuk pada bagaimana seseorang menyadari permasalahan privasi dan keamanan serta menerapkannya di jaringan sosial. Hipotesis yang menghubungkan kesadaran ini dengan kecemasan pengguna telah dinyatakan tidak mempengaruhi atau ditolak. Hasil ini sejalan dengan penelitian (Afandi, 2017; Zlatolas, 2015). Security awareness menilai tingkat kesadaran kita pada ancaman privasi dan juga perilaku keamanan yang ada. Namun hal ini hanya sebatas pengetahuan pada pengguna. Kecemasan pengguna tidak ditentukan dari seberapa besar seseorang menyadari konsep keamanan privasi melainkan melalui bagaimana seseorang dapat menggunakan kesadaran tersebut untuk mengatasi kecemasan pengguna dalam keamanan data.

Implikasi Penelitian

Internet adalah sebuah sistem komunikasi global dan platform jaringan sosial terbesar di dunia. Saat ini, jaringan sosial telah menjadi pilihan utama sebagai media komunikasi dan wadah untuk berbagi informasi. Terlepas dari manfaat, penggunaan jaringan sosial juga turut serta memberikan kecemasan terhadap keamanan data yang dibagikan. Kecemasan akan data privasi pengguna berasal dari kondisi dimana masih banyak ancaman keamanan privasi yang akan terjadi terhadap pengguna. Ancaman yang didapatkan dari tindakan membagikan informasi ini antara lain berupa pencurian identitas, blackmail dan juga personal spam (Nade, 2019).

Hasil penelitian membuktikan bahwa pengguna yang mempunyai kecemasan dalam keamanan data privasi ketika mengakses jaringan sosial (internet users' information privacy concerns) akan melakukan perilaku keamanan pada jaringan sosial (security behavior). Penelitian ini juga menjelaskan bahwa kepercayaan pengguna terhadap ancaman-ancaman dalam mengakses internet (perceive security threat) mempengaruhi tingkat kecemasan keamanan oleh pengguna dalam mengakses jaringan sosial. Penelitian ini juga memberikan kontribusi metodologi dengan membuktikan bahwa instrumen penelitian yang berasal dari studi-studi sebelumnya telah diuji valid dan dapat dibuktikan. Seiring dengan pembuktian tersebut, instrumen-instrumen dalam penelitian ini dapat digunakan untuk membantu para pengguna dan peneliti dalam memahami pandangan dan wawasan pengguna terhadap ancaman keamanan di internet, kecemasan pengguna, dan perilaku melindungi keamanan pada jaringan sosial.

Dalam implikasi praktis, studi ini memberikan pengetahuan yang lebih kepada developer jaringan sosial mengenai bagaimana kecemasan terhadap keamanan data privasi dapat mempengaruhi perilaku keamanan dari pengguna jaringan sosial. Oleh karena itu, para developer harus terus meningkatkan syarat dan ketentuan keamanan yang disediakan untuk menanggapi masalah kecemasan keamanan pengguna. Selain dapat membantu menyelesaikan kecemasan, penggunaan teori ini juga dapat membantu para developer untuk dapat lebih dipercaya oleh calon pengguna. Dalam merancang jaringan sosial, perlu diperhatikan pada bagian ketentuan bahwa ketentuan-ketentuan yang disediakan harus

dijelaskan dengan bahasa yang jelas dan transparan. Studi dan penelitian sebelumnya telah menunjukan ketentuan ini seringkali masih sulit untuk dipahami oleh para penggunanya secara keseluruhan (Wisniewski et al., 2017; Alqarni, 2018; Nade, 2019). Untuk mengurangi resiko masalah yang telah dijabarkan, para developer dapat memberikan solusi alternatif dengan memberikan ringkasan dari ketentuan-ketentuan yang dapat memungkinkan pengguna untuk mengetahui lebih dalam terhadap data yang diambil dari informasi personal pengguna.

DAFTAR PUSTAKA

[1] Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. Journal of Global Marketing, 31(2), 96–110. https://doi.org/10.1080/08911762.2017.1412552

[2] Aghasian, E., Garg, S., Gao, L., Yu, S., & Montgomery, J. (2017). Scoring Users' Privacy Disclosure Across Multiple Online Social Networks. IEEE Access, 5, 13118–13130. https://doi.org/10.1109/ACCESS.2017.2720187

[3] Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User Trust in Social Networking Services: A Comparison of Facebook and LinkedIn. Computers in Human Behavior, 69(2013), 207–217. https://doi.org/10.1016/j.chb.2016.12.013

[4] Iman, R. N., Asmiyanto, T., & Inamullah, M. H. (2020). Users' Awareness of Personal Information on Social Media: Case on Undergraduate Students of Universitas Indonesia. Library Philosophy and Practice, 2020, 1–11.

[5] Kemp, S. (2021). Digital in 2021. Digital 2021: The Latest Insights into the State of Digital. https://wearesocial.com/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital

[6] Kusyanti, A., Puspitasari, D. R., Catherina, H. P. A., & Sari, Y. A. L. (2017). Information Privacy Concerns on Teens as Facebook Users in Indonesia. Procedia Computer Science, 124, 632–638. https://doi.org/10.1016/j.procs.2017.12.199

[7] Mohamed, N., & Ahmad, I. H. (2012). Information Privacy Concerns, Antecedents and Privacy Measure Use in Social Networking Sites: Evidence from Malaysia. Computers in Human Behavior, 28(6), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008

[8] Nade, S. D. (2019). Default Privacy v / s Custom Privacy : Embodiment of Privacy by Adolescents during the Usage of Social Networking Site. IMPACT: International Jurnal, 7(2), 87–98.

[9] Soumelidou, A., & Tsohou, A. (2019). Effects of Privacy Policy Visualization on Users' Information Privacy Awareness Level: The case of Instagram. Information Technology and People, 33(2), 502–534. https://doi.org/10.1108/ITP-08-2017-0241

[10] Wijoyo, H., Limakrisna, N., & Suryanti, S. (2021). The Effect of Renewal Privacy Policy Whatsapp to Customer Behavior. Insight Management Journal, 1(2), 26–31. https://journals.insightpub.org/index.php/imj

[11] Wolf, R. De. (2020). Contextualizing How Teens Manage Personal and Interpersonal Privacy on Social Media. New Media and Society, 22(6), 1058–1075. https://doi.org/10.1177/1461444819876570

[12] Zeng, M., Lin, S., & Armstrong, D. J. (2020). Are all Internet Users' Information Privacy Concerns (IUIPC) Created Equal? AIS Transactions on Replication Research, 6(1), 3. https://doi.org/10.17705/1atrr.00046

[13] Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy Antecedents for SNS Self-Disclosure: The case of Facebook. Computers in Human Behavior, 45, 158–167. https://doi.org/10.1016/j.chb.2014.12.012

[14] Afandi, I. A., Kusyanti, A., & Wardani, N. H. (2017). Analisis Hubungan Kesadaran Keamanan, Privasi Informasi, Perilaku Keamanan Pada Para Pengguna Media Sosial Line. Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 1(9), 783–792.

[15] Zulaikhah, R. A. C., Mudjahidin, & Aristio, A. P. (2020). Analisis Faktor yang Mempengaruhi Continuance Intention pada Penggunaan Mobile Payment dengan Metode Structural Equation Modeling. INTEGER: Journal of Information Technology, 5(1), 20–29. https://doi.org/10.31284/j.integer.2020.v5i1.752