Texten nedan är ett öppet brev formulerat av forskare från Chalmers och KAU. För förfrågningar, vänligen kontakta:
The text below is an open letter formulated by a group of researchers from Chalmers University of Technology and Karlstad University. For inquiries please contact:

- Asst. Prof. **Elena Pagnin** - elenap@chalmers.se
- Prof. **Simone Fischer-Hübner -** simone.fischer-huebner@kau.se
- Dr. **Victor Morel** - morelv@chalmers.se

Svensk version, for English see below

Gemensamt uttalande från vetenskapsmän, forskare och säkerhetsutövare om de förutsebara konsekvenserna av de senaste förfrågningarna om att försvaga säkerheten i populära meddelandeappar, i enlighet med förslaget till förordning om datalagring och tillgång till elektronisk information.

I dokumentet föreslås ett nytt sätt att reglera datalagring och tillgång till ”interpersonell” digital kommunikation. Ett av de krav som ställs är att ”*Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster* [...] *ska anpassa sin verksamhet så att* ***hemliga tvångsmedel*** *kan verkställas.*” (punkt 2 på sidan 1). I synnerhet bör ”[...] *brottsbekämpande myndigheter bör ges så* ***goda förutsättningar som möjligt*** *att utföra sitt uppdrag,* [...] samtidigt som [...] *enskildas rätt till skydd för sina grundläggande* **fri- och rättigheter**” respekteras. (Avsnitt 4, sidan 32).

Vi är medvetna om att Sverige genomgår en period av särskilda hot, vilket skapar ett legitimt behov av att se över hur kommunikationstekniken har utvecklats genom åren och vilka befogenheter brottsbekämpande myndigheter bör ha för att övervaka sådan kommunikation. Vi är dock oroade över de senaste kraven som regeringen har ställt på storskaliga meddelandeappar, som tekniskt sett innebär att man antingen inför 1) skanning på klientsidan eller 2) bakdörrar i totalsträckskrypterad kommunikation. Vi skulle därför vilja dela med oss av vår åsikt om hur sådana krav förhåller sig till regeringens förslag samt de konsekvenser vi förutser om Sverige verkligen går i denna riktning.

Våra farhågor och reflektioner om det aktuella läget

Baserat på en teknisk analys av vissa rättsliga konsekvenser av förslaget presenterar vi några reflektionspunkter om det aktuella läget och förutsebara konsekvenser.

1. Vi förstår att tillgång till konversationer i realtid kan underlätta utredningar avsevärt. Att **kräva att leverantörer av totalsträckskrypterade (end-to-end encrypted) meddelandeappar ska införa bakdörrar i sina system kommer** dock **inte att lösa problemet, utan kan i stället skapa en kapprustning.** De som använder appen för olagliga syften kan helt enkelt byta till en annan app eller skapa en hemmagjord lösning för säker kommunikation, möjligtvis baserad på befintliga säkra system. Signal är en av de utvalda **totalsträckskrypterade** tjänsterna. **Signal är ett projekt med öppen källkod**, vilket innebär att koden är tillgänglig för alla. Det är därför tekniskt möjligt att skapa en säker fork (dvs. en alternativ version) av Signal, utan bakdörrar eller möjlighet till övervakning

av brottsbekämpande myndigheter. Att ta bort Signal-appen från den svenska marknaden hindrar inte brottslingar från att köra **sin egen version av Signal.** Att sätta in en bakdörr i ett meddelandesystem skulle därför faktiskt försvaga säkerheten för interpersonell digital kommunikation bland icke-kriminella personer i Sverige, **men det kommer inte att hindra organiserad brottslighet från att distribuera sin egen bakdörrsfria version**. Dessutom **slutar det inte med totalsträckskryptering**: det finns andra kända sätt att uppnå ”privat” kommunikation i ett offentligt utrymme, t.ex. steganografi. Även AI kan hjälpa till att utforma mer kreativa och oförutsedda nya medel. Aktörer som omfattas av förslaget kan mycket väl gå vidare till andra sätt att kommunicera om var de befinner sig.

2. Det som gör Signals meddelanden säkra är användningen av ett komplext kryptografiskt protokoll som kallas Signalprotokollet. _“Several closed-source applications have implemented the protocol, such as WhatsApp [...], Google Messages, [...] Facebook Messenger, [...], Skype_ ” (från wikipedia). Med tanke på att Sveriges befolkning är liten jämfört med resten av världen, och att Sverige har en ganska internationell sammansättning **, ifrågasätter vi den svenska regeringens möjlighet att kräva att bakdörrar införs** i dessa kommunikationsplattformar. Vi förutser istället att företag kan komma att föredra att dra sig ur den svenska marknaden snarare än att äventyra sina system över hela världen, vilket framgår av det uttalande som Signals VD gjorde i pressen i slutet av februari.

3. **Att kompromissa med säkra kommunikationsmedel kommer att slå slint**. Det svenska försvaret har redan tagit upp denna fråga. Oavsett vilket kommunikationssystem den svenska polisen planerar att använda, kan de vara säkra på att det verkligen är säkert och att brottslingar inte kommer att ha tillgång till ett liknande nätverk? Den senaste tidens historia visar att införandet av bakdörrar i datorsystem också gör det möjligt för illasinnade aktörer att utnyttja dessa sårbarheter. Se t.ex. dataintrånget av Salt Typhoon 2024 i USA, där en hackergrupp som tros ha drivits av Kinas ministerium för statssäkerhet drog nytta av ett avlyssningssystem som installerats i stora amerikanska telekomföretag.

4. Om ”*tillgång till uppgifter om elektronisk kommunikation på underrättelsestadiet kan vara avgörande* [...]” (Avsnitt 4, sidan 31), kan regeringen då vara öppen med *hur de planerar att* **hantera informationsmängden på ett säkert sätt och se till att den endast används för legitima ändamål**? Denna oro förefaller berättigad med tanke på de senaste skandalerna som uppdagats av enheter som innehar en enorm mängd personuppgifter, se t.ex. den senaste Uber-skandalen.

Slutsats: Att införa bakdörrar i system för totalsträckskryptering kommer att vara ett ineffektivt och olämpligt sätt att bekämpa brottslighet, eftersom brottslingar lätt kan hitta andra sätt att kommunicera privat. Å andra sidan kommer säkerhetsriskerna för industrin, samhället och individers grundläggande rätt till integritet att öka avsevärt, vilket diskuteras av professor Matthew Green i hans inlägg *Three questions about Apple, encryption, and the U.K.*

Säkra och bättre vägar framåt

Inom en rimlig rättslig ram (som föreslås i förslaget till förordning) kan åtkomst på enheten vara en lämpligare väg framåt som inte kräver någon ändring av Signal-protokollet. Det skulle därför inte

påverka några andra personer än de kriminella som är föremål för åtgärden. För att avsevärt minska risken för massövervakning och eventuella missbruk från illvilliga aktörers sida måste detta dock vara en riktad åtgärd som strikt följer rättsliga förfaranden och som under inga omständigheter bör kräva eller främja (utan snarare förhindra) ett brett genomförande av ”inbyggd tillgång till enheter”

English version

Joint statement from scientists, researchers, and security practitioners regarding the foreseeable implications related to recent requests to weaken the security of large-scale messaging apps, in accordance with the proposal for the “Data Storage and Access to Electronic Information” regulation.

The document proposes a new way to regulate data storage and access to “interpersonal” digital communication. One of the requests made is that “*Providers of number-independent interpersonal communication services* [..] *shall adapt their operations so that* ***secret coercive measures*** *can be implemented.*” (point 2 on page 1). In particular, “[..] *law enforcement authorities should be given the* ***best possible conditions*** *to carry out their mission,* [..while respecting..] *individuals’ right to protection of their fundamental* ***freedoms and rights****.*” (Section 4, page 32).

We acknowledge that Sweden is undergoing a period of special threat, which generates a legitimate need of revising how communication technologies have evolved over the years, and what powers law enforcement should have on monitoring such communication. However, we are concerned by the latest requests imposed by the government to large-scale messaging apps, which technically amounts to either introducing 1) client-side scanning or 2) backdoors in end-to-end encrypted communications. We would therefore like to share our opinion on how such requests articulate with the regulation proposal and of some consequences we foresee, would Sweden indeed proceeds in this direction.

Our concerns and reflections on the current state of affairs

In what follows, we collect some reflection points on the current state of affairs and foreseeable implications, based on a technical analysis of some legal consequences of the proposal.

1. We understand that accessing real-time conversation may considerably facilitate investigations. However, **demanding end-to-end (E2E) encrypted messaging app providers to introduce backdoors in their system will not solve the problem, and can instead create an arm race.** Those using it for illegal purposes may simply switch to another app, or create a home-brewed secure communication solution, potentially based on existing secure systems. Signal is one of the targeted end-to-end encrypted communication systems. **Signal is an open source project**, which means that the code is available to anyone. It is therefore technically possible to create a secure fork (i.e., an alternative version) of Signal, without backdoors nor possibility of law enforcement monitoring. In effect, removing the Signal app from the Swedish market does not effectively prevent malicious actors from running **their own version of Signal.** Hence, setting a backdoor in a messaging system would actually weaken the security of interpersonal digital communication amongst non-criminal people in Sweden, **but it will not prevent organized crime from deploying their own backdoor-free**

version. Furthermore, **it does not end with end-to-end encryption**: there are other known ways to achieve "private" communication in a public space, e.g., steganography, and AI can help devise more creative and unforeseen new means as well. Actors targeted by the proposal may very well move on to other means of communicating about their whereabouts.

2. What makes the Signal's messages secure is the use of a complex cryptographic protocol called the Signal Protocol. *"Several closed-source applications have implemented the protocol, such as WhatsApp [..], Google Messages, [..] Facebook Messenger, [..], Skype"* (from wikipedia). Given the small size of Sweden's population compared to the rest of the world, and its rather international composition, **we question the Swedish governments' lever to demand the introduction of backdoors** in these communication platforms. We instead foresee that companies may prefer to pull out of the Swedish market rather than compromising their systems worldwide, as seen in the statement made by Signal's CEO in the press late February.

3. **Compromising secure communication means will backfire**. The Swedish Defense has already raised this concern. Whatever communication system the Swedish Police is planning to use, can they be sure that it is truly secure and that criminals will not have access to a similar network? Recent history shows that introducing backdoors into computer systems enables the exploit of these vulnerabilities by malicious actors as well. For instance, see the 2024 Salt Typhoon hack in the USA, where a hacker group, believed to be operated by China's Ministry of State Security, benefited from a wiretap system installed in major US telecom companies.

4. If "*Access to data on electronic communication at the intelligence stage can be crucial* [..]"(Section 4, page 31), can the government be transparent on *how they plan to* **securely handle the load of information and ensure it to be used for legitimate purposes only**? This concern appears legitimate given the recent scandals emerged by entities in possession of a giant amount of personal data, see e.g., the recent Uber scandal.

Conclusion: Including backdoors in end-to-end encryption systems will be an ineffective and inappropriate means for fighting crime, because criminals can easily find other means for communicating privately. On the other hand, security risks for industry, society, and individuals' fundamental rights for privacy will significantly increase, as discussed by Prof. Matthew Green in his post on *Three questions about Apple, encryption, and the U.K.*

Secure and better paths forward

Within a reasonable legal framework (as suggested in the regulation proposal), on-device access approach could be a more appropriate way forward that does not require modifying the Signal protocol. It would therefore not impact any individuals other than the targeted criminals. However, for significantly reducing the risk of mass surveillance and possible mis-uses by malevolent actors, this must be a targeted measure strictly following legal procedures and should under no circumstance require or promote (but it should rather disallow) a broad implementation of "on-device access by design".

Signatories list below

1. Asst. Prof. Elena Pagnin — Chalmers University of Technology and University of Gothenburg
2. Prof. Simone Fischer-Hübner — Karlstad University and Chalmers University of Technology and University of Gothenburg
3. Dr. Victor Morel — Chalmers University of Technology and University of Gothenburg
4. Prof. Mikael Asplund — Linköping University
5. Prof. Dr.-Ing. Meiko Jensen — Karlstad University
6. Dr. Leonardo Horn Iwaya — Karlstad University
7. Vivi Andersson, PhD Student — KTH Royal Institute of Technology
8. Adrian Perez Keilty, PhD student — Chalmers University of Technology and University of Gothenburg
9. Prof. dr. Jaap-Henk Hoepman — Karlstad University
10. Samuel Kajava, PhD Student — Chalmers University of Technology and University of Gothenburg
11. Denis Nabokov, PhD Student — Lund University
12. Dr. Stefan Alfredsson — Karlstad University
13. Dr. Tobias Pulls — Karlstad University
14. M.Sc. Martin Bergling — RISE AB /Cybernoden
15. Dr. Marco Tiloca — RISE Research Institutes of Sweden AB
16. Dr. Christine Grosse — Luleå University of Technology
17. Dr. Apostolos Pyrgelis — RISE Research Institutes of Sweden AB
18. Jonathan Magnusson, PhD Student — Karlstad University
19. Dr. Joakim Kävrestad — Jönköping University
20. M. Sc. Andreas Aurelius — RISE Research Institutes of Sweden AB
21. Dr. Seif Alwan — Uppsala university
22. Lic. Simon Jonsson — Luleå University of Technology
23. Henrik Grasshoff, PhD Student — Karlstad University
24. Dr. Boel Nelson — Uppsala University
25. Dr. Justin Pearson — Uppsala University
26. Max Kovalenko, PhD student — Uppsala University
27. Prof. Björn Victor — Uppsala University
28. Anton Holmström — Luleå University of Technology
29. Dr. Lars-Henrik Eriksson — Uppsala University
30. Dr Johannes Borgström — Uppsala University
31. Dr. Alexander Nilsson — Lund University
32. Dr. Karl-Johan Grinnemo — Karlstad University
33. Amanda Stjerna, PhD student — Uppsala University
34. George Granberry — Chalmers University of Technology
35. Ahmed El Yaacoub, PhD student — Uppsala University
36. Docent Paul Stankovski Wagner — Lund University
37. Prof. Romaric Duvignau — Chalmers University of Technology and University of Gothenburg
38. Mohamed Hashim Changrampadi, PhD student — Chalmers University of Technology and University of Gothenburg
39. Xiuqi Zhang, PhD student — Chalmers University of Technology

40. Dr. Simon Bouget, Senior Researcher — RISE Research Institutes of Sweden AB
41. Dr. Christoph Egger — Chalmers University of Technology and University of Gothenburg
42. Prof. Carl-Johan Seger — Chalmers University of Technology and University of Gothenburg
43. Dr. Daniel Hedin — Chalmers University of Technology and Mälardalen University
44. Dr. Zeeshan Afzal — Linköping University
45. Linus Nordberg — Tor Project
46. Dr. Martin Lundgren — University of Skövde
47. Dr. Thomas Fischer — University of Skövde
48. Johan Zaxmy — University of Skövde
49. Prof. Shahid Raza — RISE Sweden | Mälardalen University
50. Anke Stüber, PhD student — Uppsala University
51. Mateen Malik, PhD student — Chalmers University of Technology
52. Prof. Leonardo Martucci — Karlstad University
53. Karim Khalil, PhD student — Lund University
54. Reethika Ambatipudi, PhD student — RISE Research Institutes of Sweden AB
55. Dr. Joel Höglund — RISE Research Institutes of Sweden AB
56. Jonas Ingemarsson — University of Skövde
57. Prof. Mathias Ekstedt — KTH Royal Institute of Technology
58. Dr. Agnieszka Kitkowska — Jönköping University
59. Dr. Roman-Valentyn Tkachuk — Blekinge Institute of Technology
60. Marcus Birgersson, PhD student — KTH Royal Institute of Technology
61. Lars Magnusson, PhD student — Linnaeus University
62. Prof. em. Louise Yngström — Stockholm University
63. Dr. Fredrik Blix — Stockholm University
64. Prof. Oliver Popov — Stockholm University
65. Dr. Roberto Guanciale — KTH Royal Institute of Technology
66. Dr. Katarina Boustedt — RISE Research Institutes of Sweden AB
67. Prof. Pontus Johnson — KTH Royal Institute of Technology
68. Hanna Ek, PhD Student — Chalmers University of Technology and University of Gothenburg
69. Alessio Cicero — Chalmers University of Technology and University of Gothenburg
70. Dr. Benjamin Eriksson — Chalmers University of Technology and University of Gothenburg
71. Lucia Lavagnino, PhD student — Chalmers University of Technology and University of Gothenburg
72. Dr. Göran Olofsson — Cybercampus Sverige
73. Julius Marozas, PhD student — Chalmers University of Technology and University of Gothenburg
74. Niklas Deworetzki, PhD student — Chalmers University of Technology and University of Gothenburg
75. Carl Magnus Bruhner, PhD student — Linköping University
76. Prof. Tobias Oechtering — KTH Royal Institute of Technology
77. M. Sc. David Olgart — KTH Royal Institute of Technology
78. Prof. Rose-Mharie Åhlfeldt — University of Skövde
79. Daniel Freiermuth, PhD Student — Chalmers University of Technology and University of Gothenburg
80. Dr. Farzaneh Karegar — Karlstad University
81. Dr. Gazmend Huskaj — Stockholm University
82. Francisco Blas Izquierdo Riera (Klondike), PhD student — KITS and Chalmers University of

Technology and University of Gothenburg

83. Dr. Magnus Almgren — Chalmers University of Technology
84. Dr. Rasmus Dahlberg — Independent
85. Prof. Gunnar Karlsson — KTH Royal Institute of Technology

— Late Signers

86. Prof. Sonja Buchegger — KTH Royal Institute of Technology
87. Dr. Joakim Brorsson — Hyker Security