4. Security uncertainty

Companies lack transparency about what they do to safeguard users' data, which means people don't know the security, privacy, and human rights risks they face when using a particular platform or service.

People entrust internet, mobile, and telecommunications companies with enormous amounts of personal information. Weak security safeguards can lead to theft or malicious exposure of this information. Companies that wish to earn and maintain user trust—and mitigate material risks to their business—should demonstrate a commitment to keeping user information secure.

The 2018 Index contains three indicators (P13, P14, P15) evaluating company transparency about what internal steps they take to keep user information secure. Companies should disclose basic information about their own internal security policies so that users can better understand the risks of using their products and services, and make informed decisions about how to use them safely.

> The Index also includes three additional security indicators evaluating company disclosure of encryption policies and practices (for internet and mobile ecosystem companies) (P16), company disclosure of what users can do to keep their accounts secure (P17), and company disclosure of materials aimed at educating users about how they can protect themselves from cybersecurity risks (P18). Companies made few substantive changes to their disclosure of the security issues addressed in these indicators. More information on how companies performed on these indicators can be found at: https://rankingdigitalrights.org/index2018/

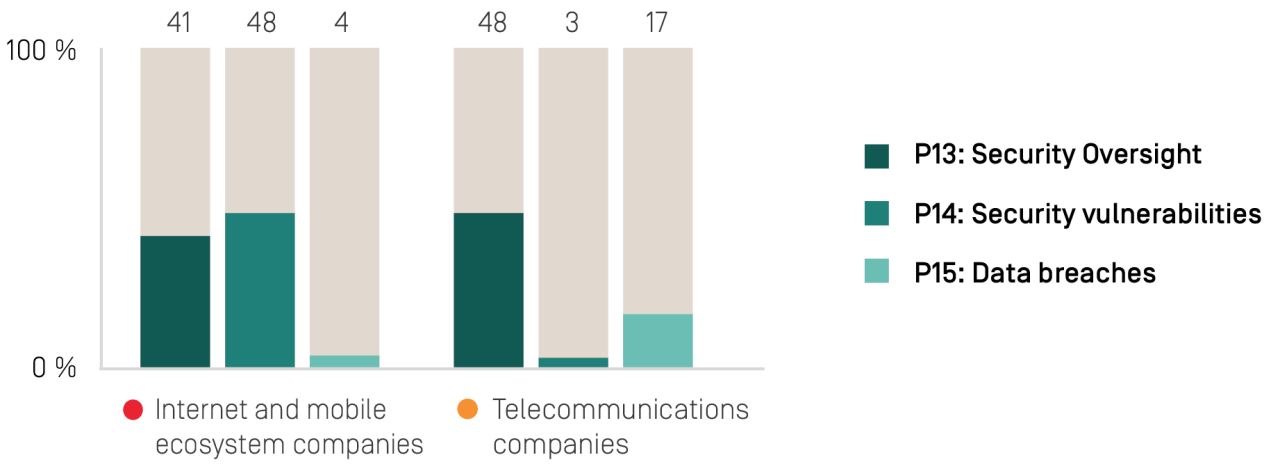
4.1. Disclosure failure ## {#section-41}

Companies fail to communicate basic information about what they are doing to keep users' information secure.

Results of the 2017 Index showed that companies tended to communicate more about what users can do to protect their own information than about what the companies themselves do to keep user data secure.[36] The 2018 Index data shows that companies have made little progress in this area.

Despite the rise in data breaches reported in the media, and growing concerns about how companies keep the vast amount of data they hold on users secure, companies across the board lacked clear and consistent disclosure of steps they take to safeguard data that they collect and store. While internet and mobile ecosystem companies disclosed more than telecommunications companies about their internal security measures, all companies fell short of providing enough information for users to know what policies and practices are in place to keep their information secure (Figure 5).

Figure 5 | How transparent are companies about their internal security measures (P13-P15)?



The 2018 Index data revealed the following trends:

- **Few companies communicate their policies for handling data breaches.** Most companies failed to provide any information at all about how they respond to data breaches (P15). While two of 22 companies—Apple and Vodafone—improved, and Vodafone was the only company to receive a full score on that indicator, most companies still failed to disclose even basic information about what procedures they have in place to respond to data breaches in the event that such incidents occur (see Section 4.2).

- **Companies do not communicate enough information about security oversight practices.** Data showed that companies lacked transparency about their security oversight procedures, including whether they limit employee access to user information. While all companies tended to disclose some information about their oversight procedures, most still fell short of clearly communicating to users what steps they take to keep their information secure (P13) (see Section 4.3).

- Nonetheless, five companies—Airtel India (Bharti Airtel), Celcom (Axiata), Etisalat UAE, Orange France, and Tencent—improved their disclosure of security oversight policies and practices (P13). Celcom (Axiata) and Orange France both made clearer commitments to conduct security audits, and Airtel India (Bharti Airtel) and Etisalat UAE published more detailed information about steps they take to limit and monitor employee access to user information. Tencent also clarified how the company limits employee access to WeChat user information, though it did not disclose any mechanisms in place to ensure these policies are enforced.

- **Companies lacked clarity about how they handle security vulnerabilities.** While internet and mobile ecosystem companies were more transparent than telecommunications companies about their processes for addressing security vulnerabilities, all companies lacked clarity about their policies and processes (P14). No company made any improvements to their disclosure of their approaches to dealing with security vulnerabilities in the 2018 Index (see Section 4.4).

4.2. Handling of data breaches ## {#section-42}

Most companies failed to disclose policies for responding to data breaches, including whether they would notify those affected.

Data breaches not only expose users to financial crimes committed by malicious hackers and cybercriminals, but other actors can exploit such breaches against at-risk communities. For example, a data breach affecting an email-service provider can expose the communications and sources of human rights activists and investigative journalists to government authorities in repressive regimes.

Companies should immediately respond to data breaches when they occur. Indicator P15 evaluates if companies disclose a commitment to notify relevant authorities and potentially affected users in the event of a breach, and if they clearly disclose what kinds of steps they will take to address the impact on users.[37] Notifying the authorities without undue delay allows officials to immediately investigate a breach, find the perpetrators, and bring them to justice. Notifying victims of breaches can help them take the necessary precautions to protect themselves, such as by changing their passwords, warning their contacts, and securing financial accounts.

However, while many jurisdictions legally require companies to notify relevant authorities or take certain steps to mitigate the damage of data breaches, companies may not necessarily be legally compelled to disclose this information to the public or affected individuals. For example, telecommunications companies in India are required to notify authorities of a data breach,[38] but there is no regulatory requirement to notify victims.

Even if there is a legal requirement to notify affected individuals, the exact definition of "affected individuals" can also vary significantly in different jurisdictions. However, regardless of whether the law is clear or comprehensive, companies that respect users' rights should clearly disclose when and how they will notify individuals who have been affected, or have likely been affected, by a data breach.

Communicating about data breaches: What do we expect companies to disclose? Indicator P15 contains three elements evaluating company disclosure of policies for responding to and communicating about data breaches.

- **Element 1: Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?** Legally, companies are often required to notify the relevant authorities when a data breach occurs. This element does not focus on whether companies disclose the specifics of which authorities they will notify, since this may vary from jurisdiction to jurisdiction, but rather whether companies commit to notify the designated authority as soon as possible.

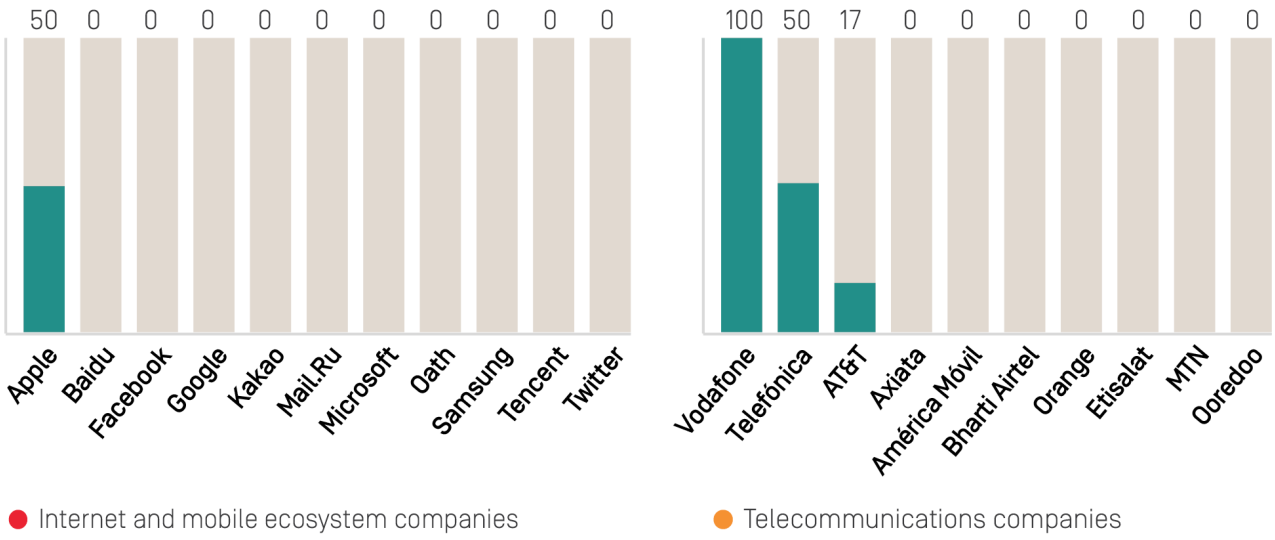
- **Element 2: Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach?** Companies should commit to notifying affected individuals as soon as possible and fully disclose what

information of theirs was exposed.

- **Element 3: Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?** Although a company's specific response will vary depending on the nature of the breach, the company should provide examples of what kinds of steps it will take internally to secure its data and commit to notifying affected individuals of steps they can take to mitigate risk or damage. See 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/#P15.

Since the 2017 Index there has been only minor progress. Apple joined AT&T, Telefónica, and Vodafone as the only companies to disclose any information about their policies and practices for responding to data breaches.

Figure 6 | How transparent are companies about policies for responding to data breaches (P15)?



As Figure 6 illustrates, most of the 22 companies in the Index failed to provide basic information about their policies for responding to data breaches:

- Vodafone was the only company to receive full credit on this indicator. The company disclosed a policy of notifying authorities without undue delay when a data breach occurs, and of notifying data subjects who might be affected. The company also clearly explained the steps taken to address the impact of a data breach on its users.

- Apple was the only internet and mobile ecosystem company to provide any information about policies for responding to a data breach. It was the only company aside from Vodafone to disclose any information about notifying authorities.

- All four companies—Apple, AT&T, Telefónica, and Vodafone—disclosed some information about their policies for notifying individuals affected. But only Apple, Telefónica, and Vodafone disclosed information about the steps they would take to address the impact of a data breach on users.

4.3. Security oversight ## {#section-43}

Most companies lack transparency about their security oversight policies and practices, including whether they limit employee access to user information.

While most data breaches can and do occur as a result of malicious actors and external threats, many also stem from poor internal security oversight.[39] Research shows that the security issues posed by so-called “insider threats” are as serious a problem as those posed by external threats.[40]

Good internal security practices therefore include restricting and monitoring unauthorized access to user information by employees. Companies should also conduct regular security audits to ensure that company security practices are properly implemented, that all software and systems are up-to-date, and that potential security vulnerabilities are addressed. A robust security audit program includes both internal and third-party audits, which can help to ensure that a company is not only meeting its own security standards but also following industry best practices.

Indicator P13 evaluates company disclosure of security oversight policies and practices for safeguarding user data.[41] We expect companies to disclose basic information on what steps they take internally to keep user information secure, including if they limit and monitor employee access to user information, and whether they conduct internal and external security audits on products and services. While we do not expect companies to disclose sensitive information that would undermine the security of these systems, or that would expose them to attacks, we do expect each company to disclose basic information about how these oversight systems function, so it is clear that the company has strong security processes in place.

Figure 7 | How transparent are companies about their security oversight processes (P13)?

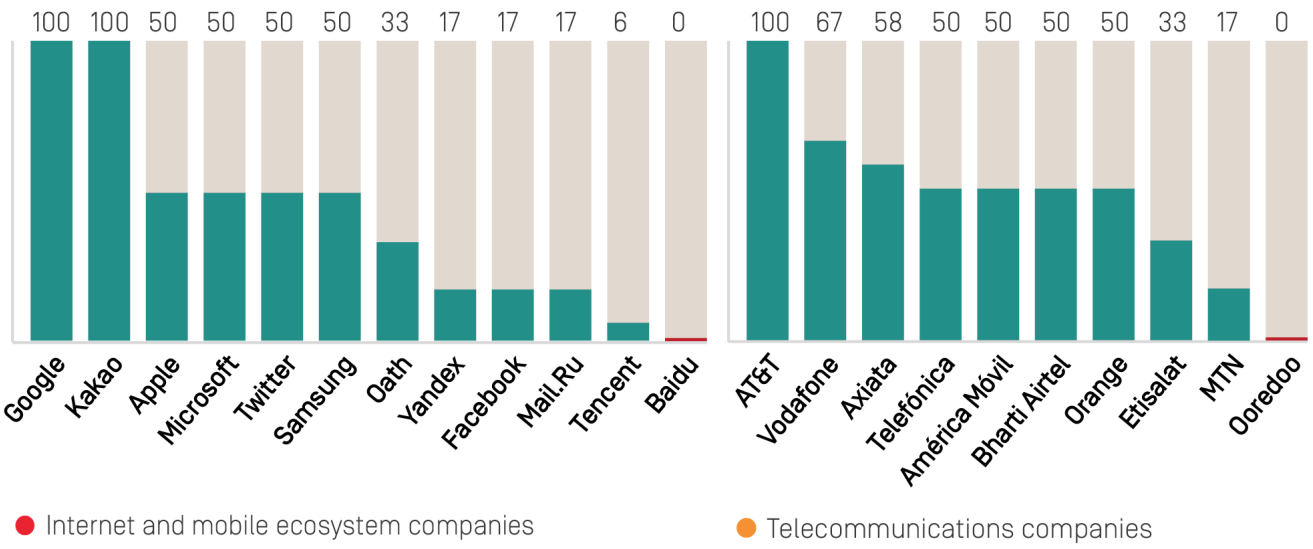


Figure 7 illustrates a wide range in companies' disclosure about security oversight processes. Notably:

- Among internet and mobile ecosystem companies, **Google** and **Kakao** earned full credit for disclosure of their security oversight processes, with each providing clear information about limiting and monitoring employee access to user information, conducting internal security audits, and commissioning third-party audits on their products and services.

- **AT&T** was the only telecommunications company to earn full credit, disclosing more than Vodafone UK, Orange France, and Telefónica Spain. The company disclosed that it conducts regular internal and external security reviews, and mentions safeguards it has in place, including limiting employee access to personal information and requiring an employee username and password to access sensitive information.[42]

- Just six companies—**AT&T, Bharti Airtel, Google, Kakao, Samsung,** and **Vodafone**—clearly disclosed that they limit and monitor employee access to user information. Six other companies, including Facebook and Twitter, failed to indicate if they have processes in place to prevent unauthorized access to user information.

- While most companies disclosed some information about internal security audits they conduct on their products and services, just four companies—**AT&T, Google, Kakao,** and **Twitter**—reported commissioning third-party security audits.

4.4. Identifying and addressing vulnerabilities

{#section-44}

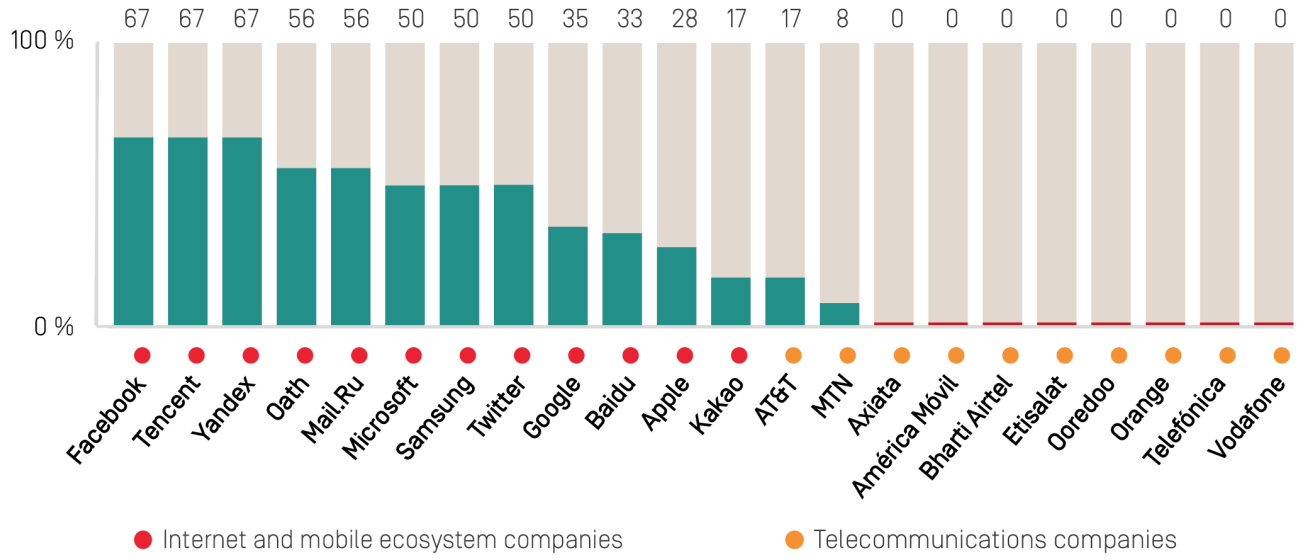
Companies lacked adequate information about how they address security vulnerabilities when they are discovered.

No security system is infallible. Even with rigorous security oversight practices in place, it is not uncommon to find vulnerabilities in a company's products and services—which, if exploited, could put their users' personal information at risk.

Indicator P14 evaluates company disclosure of how they address security vulnerabilities and what actions they take to mitigate those that they discover.[43] We expect companies to disclose that they have a program, such as a "bug bounty" to reward security researchers for alerting them to security vulnerabilities in their products. Telecommunications and mobile ecosystem companies are expected to disclose if they have made modifications to a mobile operating system and how that might affect security updates. Mobile ecosystem companies should disclose how they ensure the security of software updates and for how long they will continue to provide these updates for their operating system and other software.

As Figure 8 illustrates, all companies lacked clear disclosure of how they address security vulnerabilities.

Figure 8 | How transparent are companies about their policies for addressing security vulnerabilities (P14)?



Among internet and mobile ecosystem companies, **Facebook, Yandex,** and **Tencent** disclosed more information about how they address security vulnerabilities than their peers, although all of these companies still fell short. **Google** disclosed a security vulnerabilities reward program, but did not disclose a timeframe for responding to reports submitted for Gmail, Search, or YouTube, and did not commit to not pursue legal action against security researchers. It also failed to commit to provide security updates for its Android operating system for at least five years after release. Notably, **Apple** revealed less than Chinese internet company **Baidu**—one of the least transparent companies in the Index overall—about its approach to handling vulnerabilities it discovers.

Just two telecommunications companies—**AT&T** and **MTN**—disclosed anything about policies and practices for addressing security vulnerabilities. Notably, no telecommunications company evaluated disclosed whether they make modifications to a mobile phone's operating system.

Telecommunications companies and mobile phone manufacturers can make updates to the Android operating system code that may also delay when users can receive security updates from Google. **Samsung** is the only mobile ecosystem company evaluated that adapts for use in its devices an operating system released by another company (Samsung's implementation of Google's Android). It did not disclose a specific timeframe in which it committed to implement security updates released by Google Android. None of the telecommunications companies disclosed a specific timeframe in which mobile operating system security updates are delivered to users.

As noted in the 2017 Index report, the timely delivery of security updates is not only a security issue, but also a social equity issue, as newer and more expensive smartphones are more likely to be up-to-date than older and less expensive models, which means lower income populations can face greater security risks.[44] It is therefore crucial that companies commit to provide security patches within one month of a vulnerability being announced to the public.

4.5. Spotlight: "Bug bounties" and reporting vulnerabilities ## {#section-45}

Companies can benefit from the knowledge and skills of others, including security researchers and ethical hackers, who can identify security vulnerabilities that a company may not be aware of. If unknown to the company, security vulnerabilities can be exploited by criminals or oppressive governments seeking to spy on their citizens. In August 2016, for example, researchers at Citizen Lab identified and alerted Apple to a security vulnerability in its software that had been used to target journalists and activists in the UAE, Mexico, and elsewhere.[45] Security vulnerability reporting mechanisms are a valuable way for companies to add an extra layer of security review for their products and to demonstrate a strong commitment to user security.

By outlining clear processes for researchers to submit security vulnerabilities, companies can ensure that these reports reach the right people in a timely manner. Offering positive recognition and financial rewards ("bug bounty") is a way to further incentivize security researchers by recognizing their work, and to demonstrate that the company values these reports as part of implementing its commitment to user security.

What is a bug bounty program?

A bug bounty program is one example of a security vulnerability reporting mechanism that allows security researchers to submit "bugs," or code errors, with an emphasis on reporting security vulnerabilities that can be exploited. Bug bounty programs recognize and reward researchers for submitting these vulnerabilities, including with financial compensation. In the absence of a clearly defined vulnerability reporting mechanism such as a bug bounty program, individuals may not know how, or if, they can report these

issues to the company. This is a security liability: vulnerabilities can remain unpatched and can be exploited if discovered by malicious actors. Lack of a clear policy could also expose individuals to criminal charges of hacking or computer crimes simply for making a good faith effort to report security issues.[46] Lawsuits against journalists and security researchers for reporting vulnerabilities can also deter individuals from reporting security vulnerabilities to a company for fear of being sued or criminally charged.[47] If a company does not commit not to pursue legal charges, individuals may be discouraged from notifying a company of vulnerabilities, even through its disclosed reporting mechanism. **Further reading:** Andi Wilson, Ross Schulman, Kevin Bankston, and Trey Herr, “Bugs In the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications,” Open Technology Institute, July 2016, https://na-production.s3.amazonaws.com/documents/Bugs-in-the-System-Final.pdf.

Index data showed that all internet and mobile ecosystem companies in the 2018 Index disclosed some type of mechanism allowing researchers to report security vulnerabilities, although these programs ranged in their accessibility and comprehensiveness.

Some companies provided only an email address for researchers to submit vulnerability reports, while others offered more robust bug bounty programs that included monetary rewards and public recognition for reports submitted within the scope of the program. **Facebook** was the only company to commit not to pursue legal action against researchers who report vulnerabilities through its reporting mechanism. **AT&T** was the only telecommunications company to disclose a bug bounty program, although it did not clearly disclose a timeframe in which the company will review reports, or commit to refrain from pursuing legal action against those who submit such reports.

4.6. Recommendations for companies ## {#section-46}

- **Disclose how data breaches are handled.** Companies should disclose policies for responding to data breaches. This includes making a commitment to notify the authorities without undue delay, explaining how they will notify individuals who may have been impacted, and outlining what kind of steps they will take to address and minimize the breach’s impact.

- **Explain internal processes for safeguarding user information.** This includes disclosing that systems are in place to both limit and monitor employee access to user information, that an internal security team conducts security audits on the company's products and services, and that the company also commissions third-party security audits on its products and services.

- **Provide a mechanism for individuals to report vulnerabilities to the company.** Companies should clearly outline how security researchers can submit vulnerabilities they discover, and explain any rules they may have for these programs. Companies should also commit not to pursue legal action against individuals who submit reports of vulnerabilities within the scope of these programs.

- **Address security vulnerabilities when they are discovered.** Companies should clearly disclose the timeframe in which they will review reports of vulnerabilities. Mobile ecosystem companies and telecommunications companies that use operating systems adapted from other companies' operating systems, such as Android, should commit to provide security patches within one month of a vulnerability being announced to the public.

- **Where permitted by law, publicly commit to implement the highest encryption standards available.** This disclosure should include encryption in transit and at rest, end-to-end encryption, and forward secrecy. At minimum, companies should make it possible for users to encrypt their own data as securely as possible and communicate this to users clearly. Where the law prohibits strong encryption, companies should clearly say so to users, explaining the specific legal barrier and the potential consequences for user privacy and safety.

Footnotes

[36] 2017 Corporate Accountability Index, Ranking Digital Rights, https://rankingdigitalrights.org/index2017/assets/static/download/RDRindex2017report.pdf.

[37] 2018 Index Indictors, https://rankingdigitalrights.org/index2018/indicators/p15.

[38] "Guidelines for Protection of Critical Information Infrastructure" (National Critical Information Infrastructure Protection Centre, January 16, 2015), http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf.

[39] "2017: Poor Internal Security Practices Take a Toll," Breach Level Index (Gemalto, 2017), http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf.

[40] Christina Wood, "Insider Threat Examples: 7 Insiders Who Breached Security," *CSO Online*, March 19, 2018, https://www.csoonline.com/article/3263799/security/insider-threat-examples-7-insiders-who-breached-security.html.

[41] See 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/#P13.

[42] AT&T Privacy Policy, "What safeguards does AT&T have in place?" accessed March 20, 2018, http://about.att.com/sites/privacy_policy/full_privacy_policy.

[43] See the 2018 Index methodology at: https://rankingdigitalrights.org/2018-indicators/#P14.

[44] Nathalie Maréchal, "Global Inequality in Your Pocket: How Cheap Smartphones and Lax Policies Leave Us Vulnerable to Hacking," *Global Voices Advocacy*, March 30, 2017, https://advox.globalvoices.org/2017/03/30/global-inequality-in-your-pocket-how-cheap-smartphones-and-lax-policies-leave-us-vulnerable-to-hacking/.

[45] Nicole Perlroth, "iPhone Users Urged to Update Software After Security Flaws are Found," *The New York Times*, August 25, 2016, https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html.

[46] "Hungarian Hacker Arrested for Pressing F12," *TechCrunch*, July 25, 2017, https://techcrunch.com/2017/07/25/hungarian-hacker-arrested-for-pressing-f12/.

[47] Whittaker, Zack. “Lawsuits Threaten Infosec Research - Just When We Need It Most.” *ZDNet*, February 19, 2018, https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/.